

Avaya Integrated Management Network Management Console User Guide

November 2010

© 2010 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicate with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated by Avaya provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”). (see “Third-party Components” for more information).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without

the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Preventing Toll Fraud

“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: Introduction....11
- Intended audience....11
- Purpose....11

Chapter 2: Avaya Network Management....13
- Avaya Network Management overview....13
- Avaya Network Management terms....14
- Avaya Network Management Server....15
- Avaya Network Management Console....16
- Network maps....17
- Discovery....17
- Event handling....18
- What is new in this release....19

Chapter 3: Avaya Network Management Server....23
- Overview....23
- Starting the Avaya Network Management Server....23
- Stopping the Avaya Network Management Server....24
- Viewing the status of the Avaya Network Management Server....24
- Using Network Management Console on a Microsoft Windows operating system that supports UAC....24

Chapter 4: Avaya Network Management Console introduction....27
- Starting the Avaya Network Management Console....27
- Remote access and security....28
- Changing passwords....29
- Avaya Network Management Console user interface....29
  - Toolbar....30
  - Network Tree....32
  - Interfaces Tab....32
  - Alarms Tab....32
  - Modules Tab....32
  - Dialog area....32
  - Status Bar....33
  - Using Tooltip....33
- About read/write permission....34
  - Requesting write permission....34
- Avaya Network Management Console Options....35
  - Opening the Avaya Network Management Console's Options dialog box....36
  - SNMP Access parameters....36
  - Setting Connectivity polling parameters....40
  - Selecting a Default Map....41
  - Setting Read/Write defaults....41
  - Setting Communication Manager Server parameters....42
  - Importing Communication Manager server passwords....43
  - Exporting Communication Manager server passwords....43
  - Setting Security Banner text....44
  - Setting Syslog server parameters....45
- Status of the row in the Avaya Network Management Console table....46
- Accessing Avaya Network Management Console help....47

Chapter 5: Avaya Network Management Console Network Tree.....49
Network tree overview.....49
Viewing the network tree.....49
Subnet view.....50
Device type view.....50
VoIP system view.....51
Custom Views.....53
Printing the Network Tree.....57
Searching the Tree.....57

Chapter 6: Launching Applications.....59
Device applications that can be launched from Network Management Console.....59
Launching G860/Audio Codes Mediant 3000 EMS Client.....59
Launching Device Manager.....60
Launching IP Office Manager.....60
Launching IP Office System Status.....61
Launching Telnet.....61
Launching Web Session.....61
Pinging a device.....62
Launching an SSH session.....62
Launching Avaya Site Administration.....63
Launching Avaya MultiSite Administration.....64
Launching Avaya Fault and Performance Manager.....65
Launching Avaya Voice Announcement Manager.....65
Launching Polycom GMS.....66
Launching network-wide applications.....67

Chapter 7: Avaya Network Management Console Tables.....69
Network table.....69
Network table fields.....69
Network table colors.....71
Table toolbar buttons.....72
Choosing table parameters to display.....73
Filtering the tables.....73
Alarms table.....74
Alarms table parameters.....74
Modules table.....75
Modules table parameters.....75
Managing Objects.....75
Manually adding devices.....76
Modifying devices.....76
Device parameters.....77
Deleting devices.....78
Opening the Port Connections table.....79
Port Connections table parameters.....79
Opening the Registered Endpoints table.....80
Registered Endpoints table parameters.....80
Opening the Inventory table.....81
Inventory table toolbar.....82
Inventory table parameters.....82
Filtering the inventory table.....84

Choosing Inventory table parameters to display....84

Chapter 8: Network Maps....85
Network maps overview....85
Creating a Network Map....85
Opening a Network Map....86
Saving a Network Map to a different name....86
Printing a Network Map....86
Deleting a Network Map....87
Importing devices into the Network Map....87
Exporting the Network Map....88
CSV file structure....88

Chapter 9: Network Discovery Wizard....91
Network Discovery Wizard overview....91
Opening the Network Discovery Wizard....91
Using the Network Discovery Wizard....91

Chapter 10: Introduction to the Discovery window....97
Opening the Discovery window....97
Discovery toolbar....98
Subnets table....99
Discovery Dialog area....99
Discovery log area....100
Discovery status bar....100
Closing the Discovery window....100

Chapter 11: Discovering your network....101
Understanding the IP Discovery process....102
Setting Discovery options....103
Configuring Discovery method and range....103
Configuring the Discovery naming method....105
Selecting device types to discover....106
Scheduling network discovery....107
Discovery Scheduler field descriptions....107
Discovery of subnets and nodes....108
Discovering all subnets and nodes....108
Discovering nodes on specific subnets....109
Manually adding subnets....110
Modifying subnets....111
Subnet parameters....111
Deleting Subnets....112
Discovering interfaces....112
Using the Discovery log....113
Configuring router access parameters....113
Saving the Discovery log....114
Deleting log entries....115
Clearing the Discovery log....115

Chapter 12: Introduction to the Event Manager....117
Event Manager overview....117
Viewing the Event Manager....117

Event Manager window....118
Event log browser window....118
Event Configuration window....121
Action List window....125
Closing the Event Manager....127

Chapter 13: Managing events....129
Configuring the Event Log to discard or archive old events....129
About filtering events....130
Filtering events by security level....130
Filtering by category....131
Filtering by IP address....131
Filtering by device type....132
Filtering by acknowledged....132
Viewing all events....133
Acknowledging events....133
Removing the acknowledge mark from a event....134
Deleting events....134
Editing severity levels....134
Saving the Event table....135
Actions overview....135
Adding Actions....136
Modifying Actions....136
Action fields....137
Actions scripts....137
Action audio files....139
Deleting Actions....139
Applying changes to the Action list....139
Defining email settings for Actions that include email....140
Configuring Events....140
Assigning actions to events....140
Configuring Event Forwarding....142

Chapter 14: Introduction to the NM Log Viewer....145
NM Log Viewer overview....145
Launching the NM Log Viewer....145
NM Log Viewer window....146
NM Log Viewer toolbar....146
NM Log Viewer table....147
NM Log Viewer Status Line....148

Chapter 15: Managing Logs in the NM Log Viewer....149
Filtering logs....149
Filtering logs by security level....149
Viewing all logs....150
Exporting logs....150
Opening logs....151
Resolving the Out of Memory error....151
Closing the NM Log Viewer....152

Chapter 16: Introduction to the Quick Log Viewer....153
Quick Log Viewer overview....153

Launching the Quick Log Viewer....153
Quick Log Viewer table....154
Quick Log Viewer toolbar....154

Chapter 17: Managing logs in the Quick Log Viewer....157
Setting the number of Quick Logs to manage....157
Deleting logs....157
Clearing logs....158
Saving logs....158

Chapter 18: Introduction to the Avaya NM Backup Utility....159
NM Backup Utility overview....159
Launching the NM Backup Utility....160
NM Backup Utility window....160
NM Backup Utility toolbar....161
NM Backup Job table....162
NM Backup Utility dialog area....163
NM Backup Utility Status Line....163
Configuring the default server parameters for backup....163
NM Backup Utility Options field descriptions....164
Using the NM Backup Utility wizard....164
Editing a backup job using the NM Backup Utility....167

Chapter 19: Introduction to the Avaya NM Easy Restore Utility....169
NM Easy Restore Utility overview....169
Launching the NM Easy Restore utility....169
Restoring the data using the Avaya NM Easy Restore Utility....170
Restoring the backup file from the NM server....170
Restoring the backup file from the FTP server....170
About Recovering the PostgresSQL database using write ahead logs (WAL)....171

Appendix A: Network Management menus....173
Avaya Network Management Console Menus....173
Avaya Network Management Console File Menu....173
Avaya Network Management Console Edit Menu....174
AvayaNetwork Management Console View Menu....174
Avaya Network Management Console Actions Menu....175
Avaya Network Management Console Tools Menu....175
Avaya Network Management Console Help Menu....176
Discovery Menus....177
Discovery File Menu....177
Discovery Edit Menu....177
Discovery View Menu....178
Discovery Actions Menu....178
Discovery Help Menu....178
Event Log Browser Menus....178
Event Log Browser File Menu....179
Event Log Browser Edit Menu....179
Event Log Browser View Menu....179
Event Log Browser Help Menu....180
Event Configuration Menus....180
Event Configuration File Menu....180

Event Configuration Edit Menu....181
Event Configuration Tools Menu....181
Event Configuration Help Menu....181
Action List Menus....181
Action List File Menu....182
Action List Edit Menu....182
Action List Tools Menu....182
Action List Help Menu....182
NM Log Viewer Menus....183
NM Log Viewer File Menu....183
NM Log Viewer Edit Menu....183
NM Log Viewer View Menu....183
NM Log Viewer Help Menu....184
NM Backup Utility Menus....184
NM Backup Utility File Menu....184
NM Backup Utility Edit Menu....184
NM Backup Utility Action Menu....185
NM Backup Utility Help Menu....185

Appendix B: Enhancement introduced in previous releases....187
Enhancement introduced in Release 5.2 Service Pack 3....187
Enhancements introduced in Release 5.2 Service Pack 2....189
Enhancements introduced in Release 5.2 Service Pack 1....189
Enhancements introduced in Avaya Integrated Management Release 6.0 Service Pack 2....190

Index....195

Chapter 1: Introduction

Intended audience

This publication is for network managers who are familiar with network management and its fundamental concepts.

Purpose

This manual contains information needed to use the Avaya Network Management Console, efficiently and effectively.

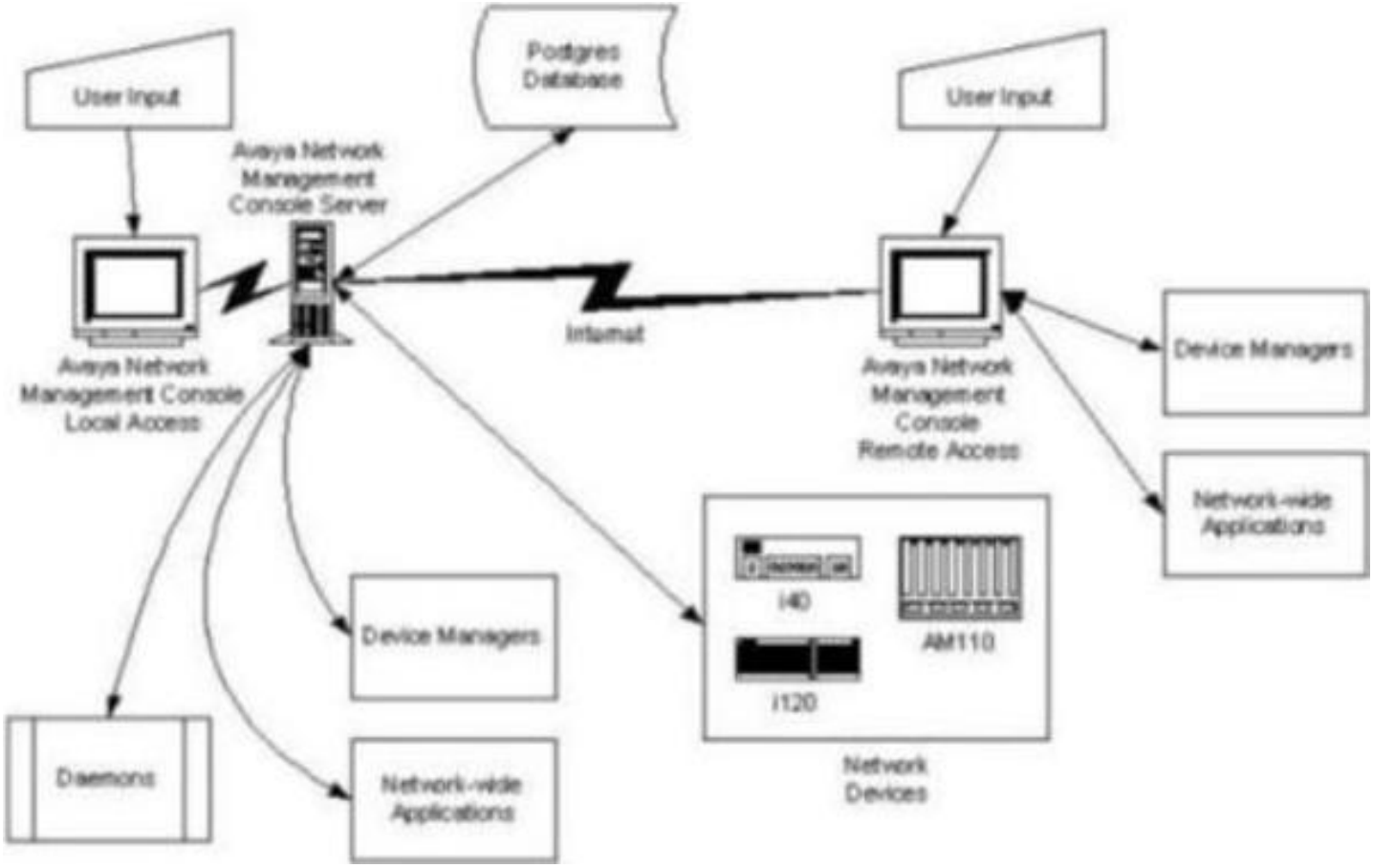
Chapter 2: Avaya Network Management

Avaya Network Management overview

The Avaya Network Management includes the Avaya Network Management Server and the Avaya Network Management Console, an application that allows you to view the devices in your network. The Avaya Network Management Console also provides a platform from which you can launch applications to manage network devices and monitor the traffic on your network. In addition, the Avaya Network Management provides a Discovery service that can search your network for devices and an Event Log that reports network events.

The Avaya Network Management uses a client/server architecture, enabling multiple users to access the Avaya Network Management Server simultaneously. Web based technology provides a method for accessing and managing your network from any computer with Internet access.

The figure below illustrates the flow of information between the different components that comprise the Avaya Network Management and the Avaya Network Management applications.



When the Avaya Network Management Server is launched, it runs a number of daemons, which poll the network devices listed in the default Network Map to determine their status and updates their colors in the Avaya Network Management Console View Area. You can manage devices or launch network-wide applications via the Avaya Network Management Console. The Avaya Network Management Console communicates these requests to the Avaya Network Management Server, which launches the correct applications. When run remotely, these applications are uploaded from the Avaya Network Management Server to the remote station.

Note:

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Avaya Network Management terms

The following list provides a list of terms used in the Avaya Network Management documentation with their descriptions.

Term	Description
Best Name	The best name for a device known to Network Management. For information on defining the method used by Network Management to arrive at the Best Name, refer to Configuring the Discovery naming method on page 105.
Branch	An intermediate level in the Network Tree. Branches include device types, subnets, and user-defined branches in custom views of the network.
Postgres Database	A database where information about the devices in the Network Map is stored.
Network Map	The set of devices that are known to the Avaya Network Management Server.
Node	A network device. Nodes include (but are not limited to) switches, hubs, routers, network printers, and computers.
Object	A branch or node in the network.
Poll	A request by an application for information from a device.

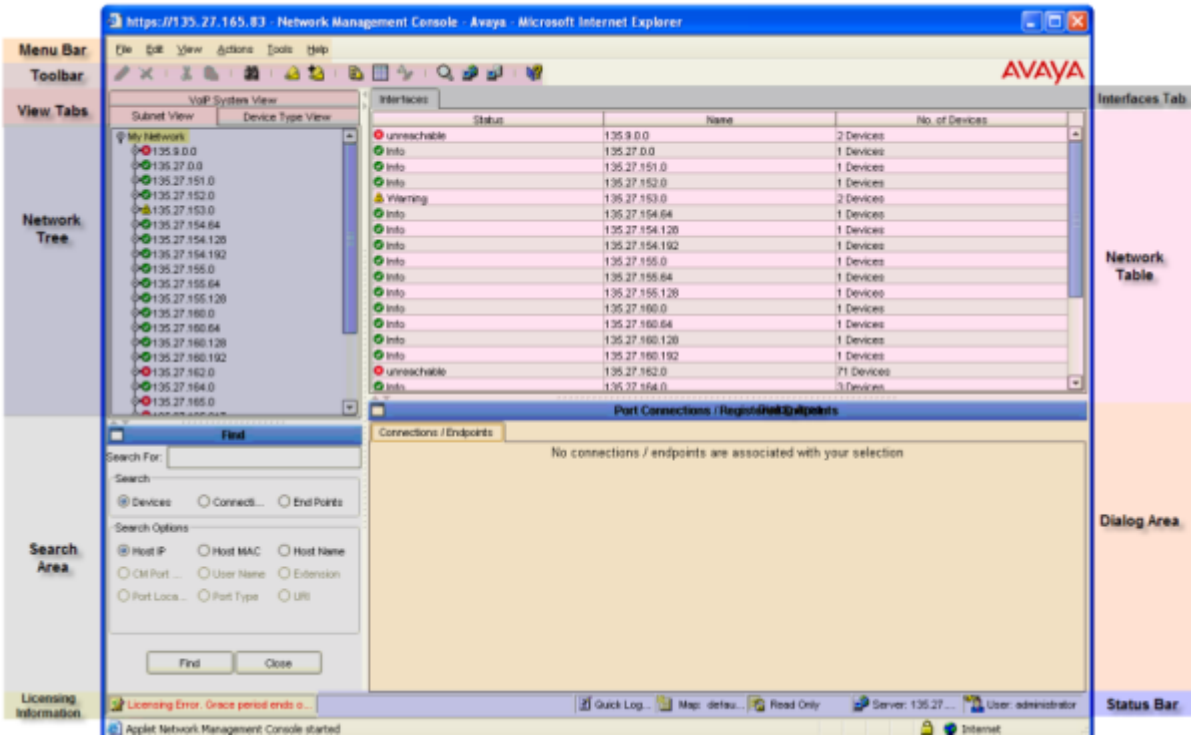
Avaya Network Management Server

The Avaya Network Management Server communicates with the devices in the network through the Simple Network Management Protocol (SNMP) V1 or V3. It receives user input through the Avaya Network Management Console and updates the Avaya Network Management Console with information from the network devices. The Avaya Network Management Server runs in the background as a Windows service. The server provides a central address for event reporting. It passes traps to the Avaya Network Management Console for display in the Event Log Browser. For more information about event handling and traps, refer to Event handling on page 18.

In addition, the Avaya Network Management Server helps you to operate the Avaya Network Management Console from a remote location. This feature provides a method for managing your network from any computer connected to the Internet. By pointing your web browser to the Avaya Network Management Server's IP address, you can access the Avaya Network Management Console and manage your network. For more information on running the Avaya Network Management Console from a remote location, refer to Starting the Avaya Network Management Console on page 27.

Avaya Network Management Console

The Avaya Network Management Console is the user interface to the Network Management Server. It receives information from the Network Management Server and sends the server information entered by the user. The AvayaNetwork Management Console displays the devices in the current Network Map using a hierarchical tree. The tree can be organized by subnet or device type, or logically by voice system hierarchy. Additionally, you can create custom views of the network.



When a device in the Network Tree is selected, information about the selected device appears in the Network Table. You can then modify the device's parameters. The AvayaNetwork Management Console also provides the ability to launch applications that communicate directly with the device. These applications allow you to manage the device through its Command Line Interface (CLI) or Device Manager, and monitor the traffic on the device. For example, if you select an Avaya G350 Device in the Network Table, you can launch Telnet to configure the device through its CLI, or launch the Avaya G350 Device Manager to configure and monitor the device through its management application. In addition, the AvayaNetwork Management Console allows you to launch network-wide applications such as, the Avaya Software Update Manager for updating embedded software.

Network maps

A Network Map consists of all of the devices known to the Avaya Network Management Server, their physical connectivity to ports, and their relationship in the voice hierarchy. The list of devices is stored in the database, along with basic information about each device. When the Avaya Network Management Console opens, the Avaya Network Management Server extracts information about the devices in the Network Map from the database. These devices are displayed in the Network Tree.

Devices can be added to the current Network Map using Discovery or the Add Device dialog box. Devices in the Network Map can also be modified. All changes to the Network Map are stored in the database.

You can maintain multiple Network Maps by saving individual maps with unique names. The Network Map whose devices are visible in the Avaya Network Management Console is the current Network Map.

Note:

Changing the map affects all open network-wide applications.

You can also create a text file that contains the necessary information about each device you want to add to the current Network Map and import the devices listed in the file into the Network Map. For more information on importing devices into the Network Map, refer to Importing devices into the Network Map on page 87.

The Avaya Network Management Server can also export the information in the current Network Map to a CSV file. For more information on exporting the device information from the current Network Map, refer to Exporting the Network Map on page 88.

Discovery

The Avaya Network Management Console uses Discovery to detect or discover your network. The Discovery tool discovers subnets and nodes, the physical port location of the devices, the Avaya VoIP hierarchy, phone information and phone locations for IP, analog and digital phones. The Discovery tool uses SNMP MIB-II on network nodes to search your network. In addition, you can instruct Discovery to use Internet Control Message Protocol (ICMP) Echo (ping) to search the network. You can instruct Discovery to search your entire network, limit the search to selected subnets, or update information about the objects in the Network View. The Discovery window displays the results of your search.

Event handling

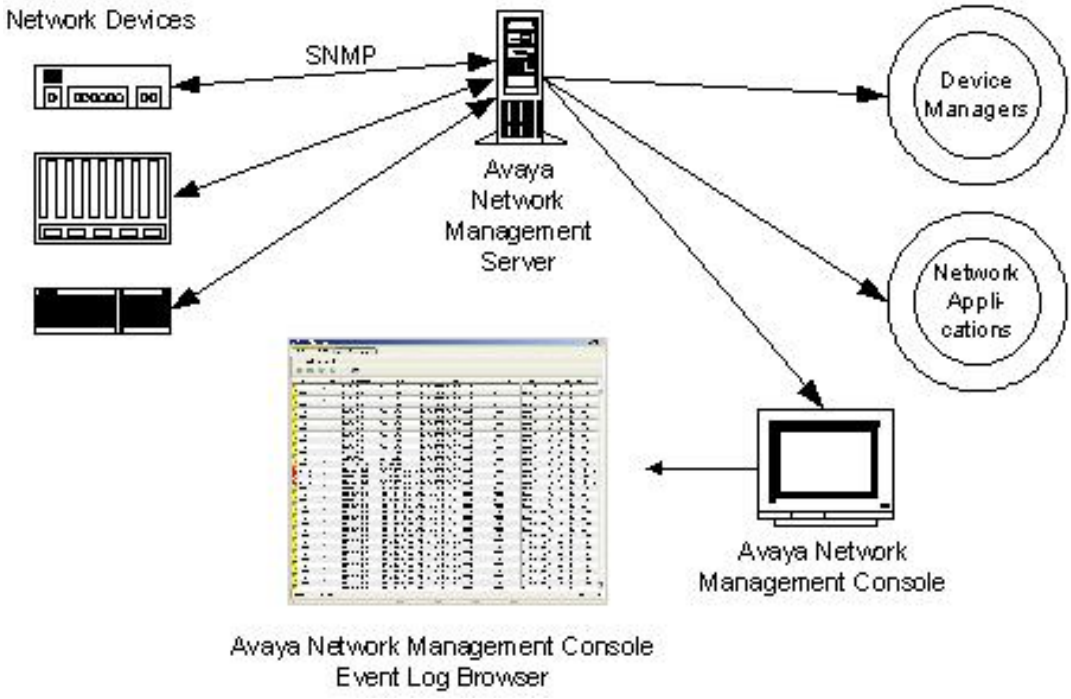
Events are unexpected or extraordinary occurrences in your network. Examples of events include the loss of a port's connection, the insertion or removal of a module from a device, and the failure of a fan or power supply. Network Management provides a method of reporting network events.

Note:

For the purposes of this topic, the terms "event" and "trap" are used interchangeably.

Network Management communicates with device agents using SNMP. Device agents can send traps to the Avaya Network Management Server reporting on the status of their ports, modules, etc. The server then passes traps to the relevant managers of the device involved and updates the Event Manager.

To receive traps using the Avaya Network Management, network devices must be configured to send traps to the oh then seAvaya Network Management Server. For information on configuring the Avaya LAN and backbone devices to send traps to the Avaya Network Management Server, refer to the *Device Manager User Guide* for the devices in your network. The Event Manager maintains a log of all traps received from the devices in the network. These traps can be viewed in the Event Log Browser.



Traps are categorized by their severity. Some traps report events that are not problems. An example of this type of trap is the insertion of a module into a device. These traps have a severity level of **Info**. Other traps require more attention, such as the loss of a regular port's connection. Traps of this type have a severity level of **Warning**. Finally, there are traps, such as the failure of a backbone link, which require immediate attention. These traps have a severity level of **Minor**, **Major**, or **Critical**.

The Event Manager displays all of the traps sent by the Avaya Network Management Server. In the Event Manager you can:

- Sort the Event log browser by any of its fields.
- Filter the traps displayed and change the severity of selected traps.
- Acknowledge traps to help you remember which traps you have already seen.
- Define the format of the description field.
- Delete traps, signifying that the problem causing the trap was resolved.

In addition, the Event Manager allows you to define event actions. Event actions can include notification through a pop-up, audio, or e-mail message or the running of a script. Actions can be assigned to any network event. You can also limit the action to events from specified sources. This feature helps you to receive immediate notification of important network events.

The Event Manager can also act as a trap surrogate, forwarding all, or selected traps to other devices.

What is new in this release

Avaya Integrated Management Network Management Release 6.0 Service Pack 2 introduces the following enhancements in the Network Management Console application.

G860 Mediant 5000

Support for the following function for G860 Mediant 5000:

Fault monitoring including Alarms Tab (RFC 3877 – ALARM MIB)

Support for the following new variant of Audio Codes gateway:

Mediant 3000 (M3K)

Support for the following functions for M3K:

- Auto discovery and manual addition
- Modify and delete operations
- Fault monitoring including Alarms Tab (RFC 3877 – ALARM MIB)

- Ping and Telnet operations

Support for Avaya Aura®Communication Manager Release 6.0.1

Avaya Integrated Management Network Management Release 6.0 introduces the following enhancements in the Network Management Console application.

- Support for Avaya Aura® Communication Manager Release 6.0.

  Network Management Console supports the following functions on Communication Manager 6.0:

  - Discovery and display of devices in the Device Type view
  - Proper correlation of devices in the VoIP System View
  - Basic administration tasks such as Adding, Deleting, and Modifying devices
  - Network Discovery Wizard

- Support for Avaya Aura® Communication Manager Release 6.0 on System Platform on the following hardware platforms:

  - S85XX
  - S8300D
  - S88XX (Next Gen)

  Network Management Console discovers the Communication Manager instance of Communication Manager running on System Platform and displays it in the Device Type view

- From this release, you do not require a license to continue using Network Management applications. As a result, WebLM is removed from the Network Management 6.0 installation. When WebLM is detected during an upgrade, the system removes it from the Network Management server.
- From this release, Network Management Console discovers the simplex and duplex servers properly. Network Management Console also displays these discovered servers properly in the VoiP System view.
- Improved encryption mechanism to connect to Avaya Aura® Communication Manager

  Currently, Network Management applications use the DES (Data Encryption Standard) encryption mechanism for ASG challenge and response used to connect to Communication Manager. From this release, all Network Management applications that connect to Communication Manager also support the use of ASG challenge and response with AES (Advanced Encryption Standard) encryption.

  As both DES and AES encryptions are supported, the application determines the encryption method to use based on the length of the challenge string

- Network Management Console polls the alarm MIB on the G860 and provides the most up-to-date and accurate information about the alarms. This enhancement has been included because the traps sent by the G860 are not reliable.

- Network Management Console can connect to a Communication Manager device using SSH. You can right-click the device listed in the View, and select SSH. You can also launch SSH from the Tools menu of Communication Manager.
- Network Management Console discovers and displays the IP500-V2 Control Unit in IP Office mode.
- You can select the family of devices to discover from the **Discovery Types** tab in the **Discovery Options** dialog box. You can select from the following available family of devices:
  - **Communication Manager**
  - **Media Gateways And Switches**
  - **IP Office**
  - **Phone**
  - **Partner Devices**
  - **Others**
- Support for IP Office Release 6.0.

  This release provides IP Office 6.0 support in the following:
  - Discovery, including VoIP SystemView
  - Port Connections
  - Secure Access Administration
  - Fault Monitoring
  - Software Update Manager
  - Provisioning and Installation Manager for IP Office
  - IP Office System Status
  - NM Backup Utility and NM Easy Restore
- Support for IP Office additional SNMP traps.

  Network Management Console’s Event Manager displays all the new traps supported in the IP Office 6.0 firmware.

Chapter 3: Avaya Network Management Server

Overview

The Avaya Network Management Server communicates with network devices. It passes information to the Avaya Network Management Console and handles requests to launch applications. In addition, the Avaya Network Management Server enables remote sessions of the Avaya Network Management Console. Ensure that the Avaya Network Management Server is running on the host computer before starting the Avaya Network Management Console locally, and that it is running on the remote server before starting a remote session of the Avaya Network Management Console.

The Avaya Network Management Server can import devices from Comma Separated Value (CSV) files into the Network Map. The Avaya Network Management Server can also export the Network Map to a CSV file, for use with other applications, such as a Microsoft Excel.

Starting the Avaya Network Management Server

The Avaya Network Management Server is a Windows Service. When Windows starts on the server station, the Avaya Network Management Server starts automatically. Using the Windows' Service Manager, you can configure the Avaya Network Management Server so that it does not start automatically.

If the Avaya Network Management Server is shut down, you have to start it manually. To manually start or stop the Avaya Network Management Server, you must be logged in to Windows with Administrator privileges. When you log off the computer, the Avaya Network Management Server continues running.

To start the Avaya Network Management Server:

Select **Start** > **Programs** > **Avaya** > **Start Avaya Services**.

Stopping the Avaya Network Management Server

To stop the Avaya Network Management Server:

Select **Start** > **Programs** > **Avaya** > **Stop Avaya Services**.

Viewing the status of the Avaya Network Management Server

To view the status of the Avaya Network Management Server:

Select **Start** > **Programs** > **Tools** > **Avaya Network Management Server Status**.

Using Network Management Console on a Microsoft Windows operating system that supports UAC

Prerequisites

If you are using Network Management Console on a Microsoft Windows operating system that support User Access Control (UAC), follow the instructions given below. If you need more information on UAC, visit the Microsoft Windows website. You can use the following Microsoft Windows operating systems that support UAC as Network Management client operating systems.

- Microsoft Windows 2008
- Microsoft Windows 7 Professional
- Microsoft Windows 2008 R2
- Microsoft Windows Vista

Note:

Network Management Console uses applications like Telnet Client which are provided along with the operating system. You need to configure it in Windows operating system before using it. To use the Telnet Client, you need to enable it from the **Control Panel**. On the Microsoft Windows operating system, you can use the Windows Features tool to install optional components.

To install Telnet Client do the following:

1. Click **Start**, and then click the **Control Panel**
2. On the Control Panel Home page, click **Programs**.
3. In the **Programs and Features** section, click **Turn Windows features on or off**.
4. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
5. In the **Windows Features** list, select **Telnet Client**.
6. Click **OK**.

   In Microsoft Windows operating systems you must run some of the Network Management Console applications as **Run as administrator**. For example, when you select **Start Avaya services**, **Stop Avaya services**, or Network Management Console Easy Restore from the start menu, right-click and then select **Run as administrator**

   Note:

   You can configure NM Easy Restore to automatically run as administrator each time you start it. To configure, you can use the procedure described in the Web site, http://support.microsoft.com/kb/922708 or refer to any Microsoft Windows Operating System documentation on UAC.

   You must set the proper Compatibility mode for the application to run as administrator by default.

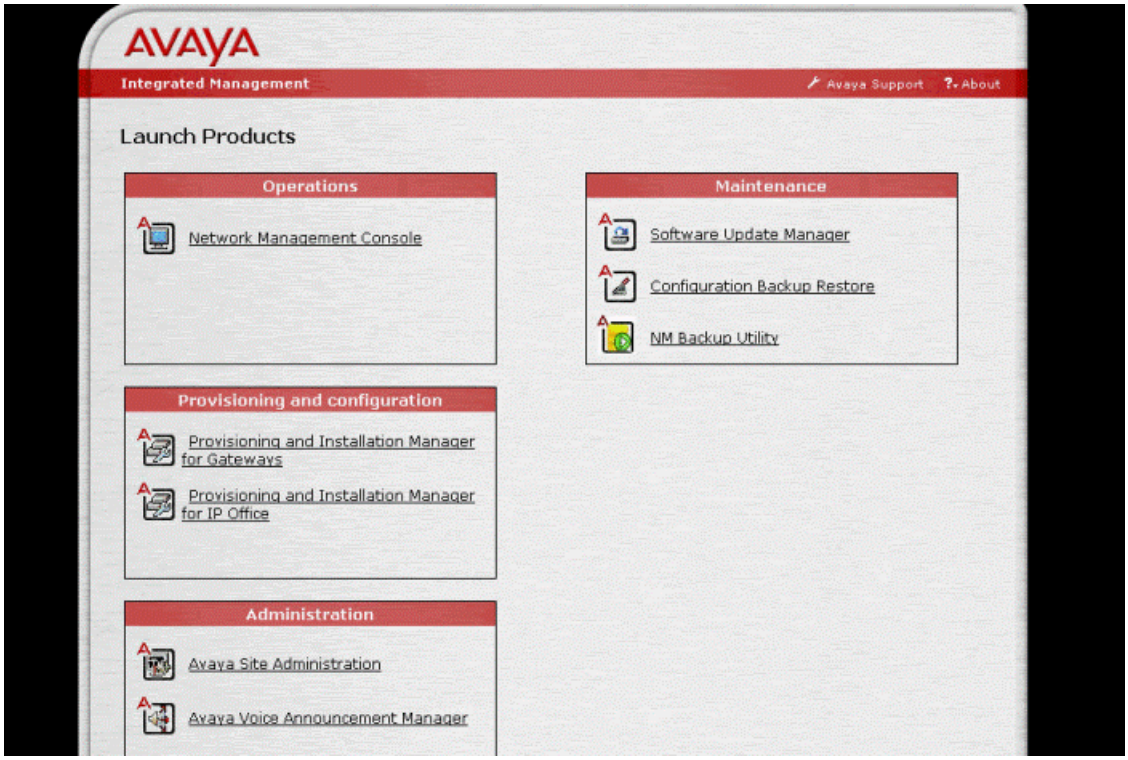
Chapter 4: Avaya Network Management Console introduction

Starting the Avaya Network Management Console

The Avaya Network Management Console is a java applet running in a browser. When you point your browser to the Avaya Network Management Server's IP address, a Java applet prepares your browser to communicate with the Avaya Network Management Server. A welcome screen opens, followed by a password screen. Once you enter a valid user name and password, the Avaya Network Management Console opens in a special browser window.

To start Network Management Console:

1. Do one of the following:
   a. To start a local session of the Network Management Console from the server, double-click the **Avaya Integrated Management** link on the Windows desktop. The Avaya Integrated Management home page is launched.
   b. To start a session of the Network Management Console from a client machine, point your web browser to `http://` *IP_Address*, where *IP_Address* is the IP address of the Network Management Server. The system displays the Avaya Integrated Management home page.



2. From the Avaya Integrated Management home page, click the **Network Management Console** link to launch Network Management Console.
3. The system displays a window requesting your user name and password.
4. Enter your user name and password, and click **OK**. The system displays the Network Management Console window.

Remote access and security

You can access the Avaya Network Management Console from any computer, using a web browser. The web server is configured to work with HTTPS, and login to the Avaya Network Management Console requires authentication. This allows only authorized users to access the Avaya Network Management Console remotely.

The Avaya Network Management Console communicates with devices using SNMP. Only the SNMPv3 protocol is encrypted and requires authentication. It is, therefore, highly recommended that you use the SNMPv3 protocol.

Changing passwords

You can change the password of logged in user through the Network Management Console.

To change the password of logged in user:

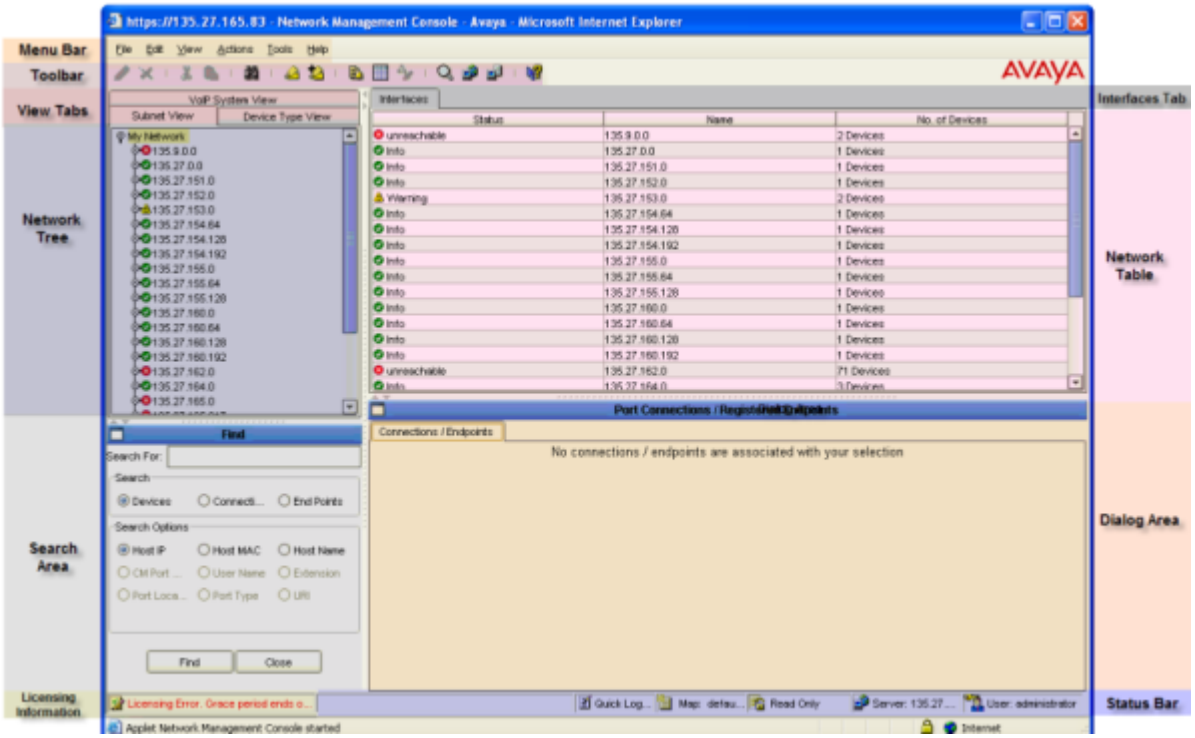
1. Select **Actions** > **Change Password**. The system displays the Password Change dialog box.
2. Enter your old password in the **Old Password** field.
3. Enter your new password in the **New Password** field.
4. Enter your new password in the **Confirm Password** field.
5. Click the **Save Changes** button..

Avaya Network Management Console user interface

The user interface consists of the following elements

- Menu bar - Menus for accessing the AvayaNetwork Management Console management functions.
- Toolbar on page 30 - Toolbar buttons for accessing the AvayaNetwork Management Console management functions.
- Network Tree on page 32 - A resizeable window containing a hierarchical representation of the Network Map.
- View Tabs - Tabs for switching between the various views of the network.
- Interfaces Tab on page 32 - Displays a table where details about the branches and nodes in the Network Tree are displayed.
- Alarms Tab on page 32 - Displays a table where alarms reported for devices on the network are displayed.
- Modules Tab on page 32 - Displays a table where a list of modules and the module type are displayed.
- Dialog area on page 32 - A resizeable window where all dialog boxes open.
- Status Bar on page 33 - Displays information about the current AvayaNetwork Management Console session.

The following figure shows the user interface, with its various parts labeled.



To resize the three main areas of the user interface, the Network Tree, the Network Table, and the Dialog Area, use the splitter bars and their arrows.

Related topics:

[Toolbar](#) on page 30
[Network Tree](#) on page 32
[Interfaces Tab](#) on page 32
[Alarms Tab](#) on page 32
[Modules Tab](#) on page 32
[Dialog area](#) on page 32
[Status Bar](#) on page 33
[Using Tooltip](#) on page 33

Toolbar

The Toolbar provides shortcuts to the main Network Management Console functions.

The table below describes the buttons on the toolbar and gives the equivalent menu options.

Button	Description	Menu Item
	Opens the Modify dialog box for the selected object.	**Edit** > **Modify**
	Deletes the selected object from the Network Map.	**Edit** > **Delete object**
	Cuts the selected object from a custom view to the clipboard.	**Edit** > **Cut object**
	Pastes the object from the clipboard into a custom view.	**Edit** > **Paste object**
	Opens the Find dialog box.	**Edit** > **Find**
	Opens the Port Connections/Registered Endpoints Table.	**View** > **Connections/ Endpoints**
	Opens the Inventory Table.	**View** > **Inventory**
	Opens the Event Manager.	**Actions** > **Event Manager**
	Opens the NM Log Viewer.	**Actions** > **NM Log Viewer**
	Opens the Discovery window.	**Actions** > **IP Discovery**
	Launches the device manager for the selected device.	**Tools** > **Avaya Device Manager**
	Launches a web session to the selected device.	**Tools** > **Web**
	Launches a Telnet session to the selected device.	**Tools** > **Telnet**
	Launches an SSH session to the selected device.	**Tools** > **SSH**
	Opens context-sensitive help.	**Help** > **Help On**

When you place the cursor on a toolbar button for one second, a label appears with the name of the button.

Network Tree

The Network Tree shows a hierarchical representation of the subnets in the Network Map or a representation of the Network Map grouped by device type or logically organized by voice system hierarchy. You can also create customized views of the Network Map.

Interfaces Tab

The **Interfaces** tab displays the Network table. The Network table provides details of the subnets, device types, or devices under the selected branch of the tree. For more information about the Network table, refer to Avaya Network Management Console Tables on page 69.

Alarms Tab

The **Alarms** tab displays a list of alarms reported by the device selected in the Network Tree. The **Alarms** tab is only enabled for devices supporting alarms. The **Alarms** tab displays current problems, faults associated with any device displayed, and severity. For more information about Alarms, refer to Table toolbar buttons on page 72.

Modules Tab

The **Modules** tab displays a list of modules and the module type that are part of the Media Gateway/Carrier. Module index. For more information about the Modules table, refer to Modules table on page 75.

Dialog area

The area under the Network table is where all dialog boxes open. This area can be resized by dragging the horizontal splitter bar with the mouse. When a dialog box opens, it replaces the current dialog box open in the Dialog area.

Status Bar

The Status Bar provides information about the Avaya Network Management Console session. It includes the following information

- Name of the open map.
- Read/Write mode of the Avaya Network Management Console.
- IP address/Name of the Network Management Server.
- Quick Log Viewer option.
- Current user Logged in to the Avaya Network Management Console.

Using Tooltip

The Network Management Console includes a Tooltip feature, which allows you to display additional information about devices in the Network map.

To use Tooltip:

1. Select **View** > **Tooltip.**
2. Place the cursor on the device's icon in the Network tree or Network table to display additional information about a device. After about one second, the Tooltip appears. The Tooltip provides the following information about the device:
   - **Name** — The Best Name of the device.
   - **Mask** — The device's IP subnet mask.
   - **MAC** — The device's MAC address
   - **Type** — The device type
   - **Interface Number** — The interface number of the displayed IP address of this device.
   - **Management Status** — The device's management status. This can be either **Managed** or **Unmanaged**.

   Tooltips for Carriers provide the following information:
   - **Building** — The building in which the carrier is physically located.
   - **Floor** — The floor on which the carrier is physically located.
   - **Room** — The room in which the carrier is physically located.

About read/write permission

There are two levels of permissions for users logging into the Network Management Console:

- Read-only - You are able to view the network and devices, but are unable to make changes.
- Read/Write - You are able to both view and make changes to the network and devices.

The following are the assigned permissions at login:

- No read/write console exists - read/write permission is automatically assigned to your console.
- Read/Write console currently exists - your console is assigned read only permission.

Note:
Only one console may have read/write permission at any given time.

If your console is opened with read only permission, you can request write permission. The console that currently has read/write permission receives a request from the Network Management Console to release the write permission. There is an allotted amount of time in which the console with read/write permission must respond to the request. If the console with read/write permission agrees to the request, or does not refuse the request in the allotted amount of time, the read/write permission is transferred to the requesting console automatically.

For instructions on setting the Timeout value, see Setting Read/Write defaults on page 41.

All functionality is supported for a console with read/write permission. This is true whether you are running the Avaya Network Management Console locally or remotely.

All functions that update the server (i.e., adding and removing a device from the map, or running a discovery process) are disabled on a console with read only permission and all update commands are inactive. If an update dialog box is open while the console is losing write permission, the Apply button of the dialog box becomes inactive until write permission is restored. This also applies to the trap manager.

Related topics:

Requesting write permission on page 34

Requesting write permission

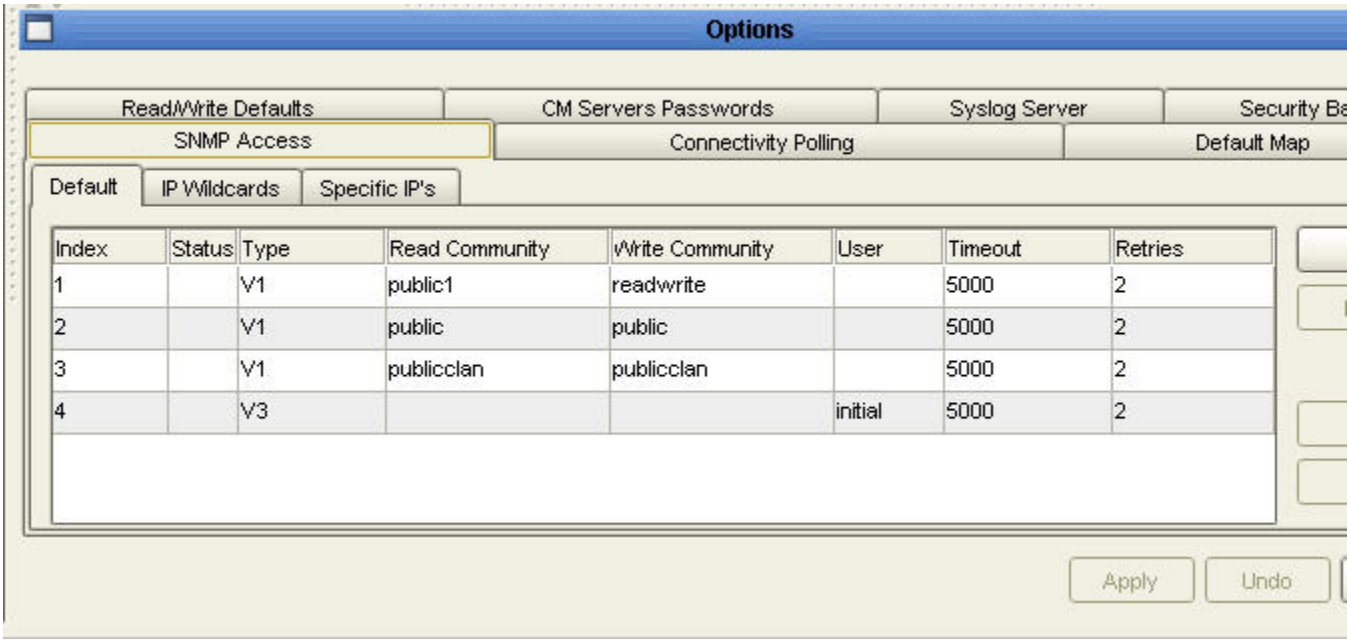
You can perform the following tasks:

1. To request read/write permission:
   a. Select **Actions** > **Get Write Permission**. The system displays the Write Permission Request dialog box.
   b. Click **OK**.
   c. If the console that currently has write permission agrees to your request, the system displays the Write Permission Received dialog box. Click **OK** to receive write permission.
   d. If the console that currently has write permission refuses your request, the system displays the Write Permission Refused dialog box. Click **OK** to proceed with read only permission.
2. If your console currently has read/write permission and a request is made for write permission by another console, the system displays the Remote Request dialog box. Do one of the following:
   a. To release read/write permission in response to another console's request, click **OK**.
   b. To refuse write permission to the requesting console, click **Refuse**.

   Note:
   If you don't click **OK** or **Refuse** before the Timeout value expires, write permission is automatically released to the requesting console.
3. To release read/write permission without a direct request from another console, select **Actions** > **Release Write Permission**.

Avaya Network Management Console Options

You can use the AvayaNetwork Management Console's Options dialog box to set the parameters such as SNMP access parameters, Connectivity polling parameters, Read/Write parameters, Communication Manager server parameter, Syslog server parameter, Default map, and Security banner text parameters.



Related topics:

[Opening the Avaya Network Management Console's Options dialog box](#) on page 36
[SNMP Access parameters](#) on page 36
[Setting Connectivity polling parameters](#) on page 40
[Selecting a Default Map](#) on page 41
[Setting Read/Write defaults](#) on page 41
[Setting Communication Manager Server parameters](#) on page 42
[Setting Security Banner text](#) on page 44
[Setting Syslog server parameters](#) on page 45

Opening the Avaya Network Management Console's Options dialog box

To open the AvayaNetwork Management Console Options dialog box:

Select **File** > **Options**. The system displays the Options dialog box.

SNMP Access parameters

Using the **SNMP Access** parameters tab of the Network Management Console Options dialog box, you can set basic SNMP parameters for specific devices, ranges of devices, and all

unspecified devices. The Network Management Server recognizes the following SNMP protocols: V1 and V3. SNMP access parameters for SNMP V1 include read and write community properties. For SNMP V3, the SNMP access parameters include a user name defined in the Secure Access Administration. For both versions of SNMP, access parameters include timeout and retry values. Each of the three tabs in the SNMP Access parameters page helps you set SNMP access parameters for different groups of devices.

- Default — To configure all devices with IP addresses not included in the other tabs.
- IP Wildcards — To configure SNMP access parameters for devices whose IP addresses fall in a specified range and not in the Specific IP's tab.
- Specific IP's — To configure SNMP access parameters for specific devices.

When polling a device, the Network Management Server uses the device's SNMP access parameters. The server first checks the Specific IP's list. If the device is listed in the Specific IP's list, the SNMP access parameters for the specific device are used. If not, the server checks the IP Wildcards list. If the device's IP address is in any of the ranges listed in the IP Wildcards list, the SNMP access parameters for the matching range are used. If the device's IP address does not match any of the ranges in the IP Wildcards list, the default SNMP access parameters are used.

Related topics:

Configuring default SNMP access parameters on page 37
Setting SNMP Access parameters for IP ranges on page 38
Setting specific IP parameters on page 39

Configuring default SNMP access parameters

The Default table lets you configure multiple default SNMP communities.

If no Specific IP definition and IP Wildcards match the IP address to be polled, the Network Management Server tests the addresses of the devices against the list of definitions in the Default list. The order of the list in the table is important, because the SNMP access parameters of the first rule in the list that matches a device's SNMP access parameters are used for that device.

To view the list of default SNMP access parameters, click the **Default** tab on the SNMP Access page of the Options dialog box. The system displays the Default table.

Do one of the following:

- To add a new set of SNMP default parameters to the list:
    i. Click **Add**. A new row opens in the **Default** table.
    ii. Select **V1** or **V3** from the **Type** drop-down list.
    iii. If you selected **V1** in the **Type** field, enter Read and Write community values in their respective fields.

iv. If you selected **V3** in the **Type** field, select a user name from the **User** drop-down list. The user name must be defined in the Secure Access Administration application. For more information, refer to the *Avaya Secure Access Administration User Guide*.

v. Enter a number in the **Timeout [ms]** field for the number of milliseconds the Network Management Server waits for a response when polling a device.

vi. Enter a number in the **Retries** field for the number of times the Network Management Server tries to poll a device.

vii. Click **Apply** to add the new default SNMP parameters definition to the Default table.

- To change the position of a row in the Default table:

  i. Select a row.

  ii. Click the arrows to move the row up or down in the table.

  iii. Click **Apply** to save the new row position.

- To edit entries in the Default table:

  i. Click the field you want to edit.

  ii. Edit the information in the field.

  iii. Click **Apply** to save the changes in the table.

- To remove a range from the Default table:

  i. Select a range.

  ii. Click **Delete**.

  iii. Click **Apply** to delete the range from the Default table.

Setting SNMP Access parameters for IP ranges

The **IP Wildcard** tab lets you to configure SNMP access parameters for ranges of devices. The Network Management Server tests the IP address of devices to poll against the list of devices in the IP Wildcards list. If the IP address matches a range, the server uses the range's SNMP access parameters when polling the device. The order in the list is important, because the SNMP access parameters of the first range in the list that matches a device's IP address are used for that device.

To view SNMP access parameters for IP ranges, click the **IP Wildcard** tab on the SNMP Access page of the Avaya Network Management Console Options dialog box. The system displays the IP Wildcard table.

Do one of the following:

- To add a new IP range to the list:
    i. Click **Add**. A new row opens in the IP Wildcards table.
    ii. Select **V1**, or **V3** from the **Type** drop-down list.
    iii. Enter an IP Wildcard in the **IP Wildcard** field.
    iv. If you selected V1 in the **Type** field, enter read and write community values in their respective fields.
    v. If you selected V3 in the **Type** field, select a user name from the **User** drop-down list. The user name must be defined in the Secure Access Administration application. For more information, refer to the *Avaya Secure Access Administration User Guide*.
    vi. Enter timeout value in the **Timeout** field
    vii. Enter the number of attempts to connect in the **Retries** field.
    viii. Click **Apply** to add the new range to the IP Wildcards table.
- To change the position of a row in the IP Wildcards table:
    i. Select a row.
    ii. Click the arrows to move the row up or down in the table.
    iii. Click **Apply**.
- To edit entries in the IP Wildcards table:
    i. Click the field you want to edit.
    ii. Edit the information in the field.
    iii. Click **Apply** to save the changes in the table.
- To remove a range from the IP Wildcards table:
    i. Select a range.
    ii. Click **Delete**.
    iii. Click **Apply** to delete the range from the IP Wildcards table.

Setting specific IP parameters

To view SNMP access parameters for specific devices, click the **Specific IP's** tab on the SNMP Access page of the Options dialog box. The system displays the Specific IP's table.

Do one of the following:

- To add a new device to the list:
    i. Click **Add**. A new row opens in the Specific IP's table.
    ii. Select V1 or V3 from the **Type** drop-down list.
    iii. Enter the device's IP address in the **IP** field.
    iv. If you selected V1 in the **Type** field, enter read and write community values in their respective fields.
    v. If you selected V3 in the **Type** field, select a user name from the **User** drop-down list. The user name must be defined in the Secure Access Administration application. For more information, refer to the *Avaya Secure Access Administration User Guide*.
    vi. Enter **Timeout** and **Retries** values in their respective fields.
    vii. Click **Apply** to add the device to the Specific IP's table.
- To edit entries in the Specific IP's table:
    i. Click the field you want to edit.
    ii. Edit the information in the field.
    iii. Click **Apply** to save the changes in the table.
- To remove a device from the Specific IP's table:
    i. Select a device.
    ii. Click **Delete**.
    iii. Click **Apply** to delete the device from the Specific IP's table.

Setting Connectivity polling parameters

Connectivity polling parameters determine whether the Network Management server use PING to determine the status of devices that do not support SNMP, the interval between PINGs, and the number of times that Network Management Server unsuccessfully PINGs a node before declaring it to be unreachable.

To set default connectivity polling parameters:

1. Click the **Connectivity Polling** tab at the top of the Options dialog box. The system displays the Connectivity Polling options.
2. Select one of the following **Connectivity Status**.

- **On** — means that devices are PINGed.
- **Off** — means that devices are not PINGed.

3. Enter a number in the **Retries** field. This is the number of times Network Management Server unsuccessfully PINGs a node before declaring it to be unreachable.
4. Enter a number in the **Timeout** field. This is the number of milliseconds Network Management Server waits for a response when PINGing a node before declaring it to be unreachable.
5. Enter a number in the **Interval** field and select either **minutes**, or **seconds**. This is the amount of time between PINGs.
6. Click **Apply** to configure the network with the new connectivity polling parameters.

Note:
To return the values to the default settings, click **Default**.

Selecting a Default Map

The **Default Map** tab of the Network Management Console Options dialog box enables you to select the Network Map that is used when the Network Management Server starts. This is useful if there are multiple Network Maps and you want to open a particular map when the Network Management Server starts.

To select a default Network Map:

1. Click the **Default Map** tab at the top of the Options dialog box.
2. Select a Network Map from the **Default map name** drop-down list.
3. Click **Apply**. The selected map is now the default Network Map.

Setting Read/Write defaults

The **Read/Write Defaults** tab of the Network Management Console's Options dialog box helps you set the default read/write permissions.

To set read/write defaults:

1. Click the **Read/Write Defaults** tab at the top of the Options dialog box . The system displays the Read/Write Defaults defaults options.
2. Select **Allow Read/Write request** to allow a user to request read/write permission. If this option is not selected, then the first console opened receives read/write permission. Any other console window that requests read/write permission is refused.
3. Enter the interval of time in seconds in the **Timeout (sec)** field that the holder of the read/write permission is allotted to respond to the read/write request.
4. Click **Apply**.

Setting Communication Manager Server parameters

The **CM Servers Passwords** tab of the Network Management Console's Options dialog box lets you set the login parameters to connect to Communication Manager servers in your network.

Note:

To discover analog, digital or IP phones, you must add the relevant Communication Manager Login parameters to the table.

To set Communication Manager server login parameters:

1. Click the Communication Manager **Servers Passwords** tab at the top of the Options dialog box.

   The system displays the Communication Manager Servers Passwords table.
2. Click **Add** to add a new Communication Manager server with which you wish to connect.
3. Select **Discover Phones** if you want to discover IP and analog phones for this Communication Manager. The state of this check box does not affect Software Update Manager's operation.
4. Enter the IP address of the Communication Manager server.
5. Enter the login ID and password to access the Communication Manager server.
6. Enter the ASG key, if ASG encrypted login is used.
7. Select the encrypted login method.

Possible values are ASG, and SSH .

8. Click **Apply**.

Result

Note:
The ASG key is a 20-character octal code, the 19th character of which must be either 0, 2, 4, or 6, and the 20th character of which must be 0.

Importing Communication Manager server passwords

Communication Manager server passwords can be imported using the **CM Server Passwords** tab. You can import the Communication Manager server passwords from a Comma Seperated Value (CSV) file.

1. Click the **CM Servers Passwords** tab at the top of the **Options** dialog box.
2. Click **Import**.
   The system displays the standard file browser.
3. Browse to the CSV file.
4. Click **Open**.
   The system displays a dialog box with a warning that all the existing rows will be deleted.
5. Do one of the following:
   - Click **Yes** to remove the existing rows and import the CSV data.
   - Click **No** to retain the existing rows and not import the CSV data.

Note:
You must click **Apply** for the changes to take effect after import.

Exporting Communication Manager server passwords

The Communication Manager server passwords can be exported to a CSV file for use with external applications or for having a backup copy.

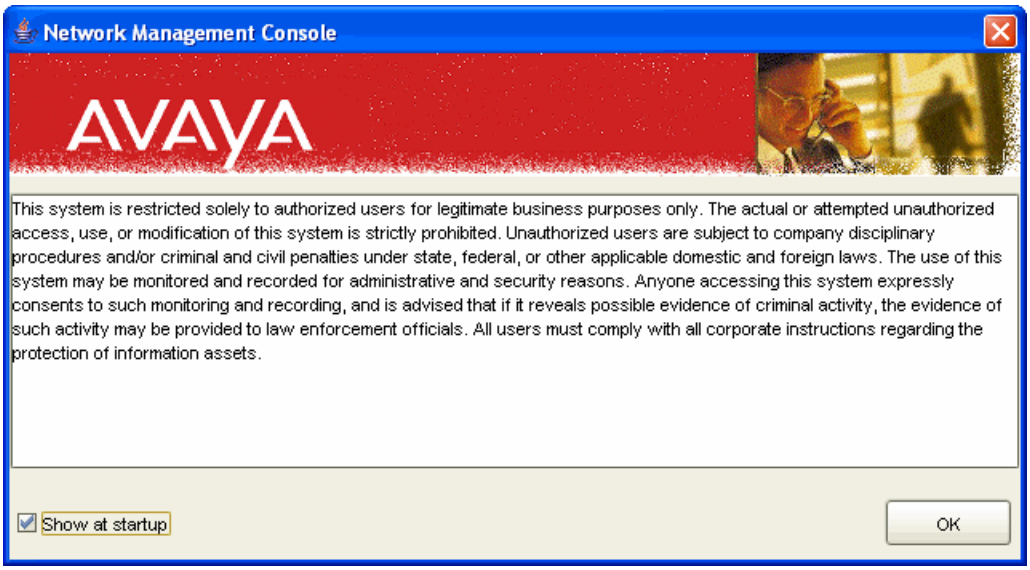
1. Click the **CM Servers Passwords** tab at the top of the Options dialog box.

The system displays the CM Servers Passwords table.

2. Click **Export**.
   The system displays the standard file browser.
3. Browse to the directory where you want to save the file.
4. Enter a name for the CSV file in the **Name** field.
5. Click **Save** to export the Communication Manager server passwords to the specified CSV file.

Setting Security Banner text

The Security Banner is launched once the Network Management Console applet is loaded.



The **Security Banner** tab of the Network Management Console's Options dialog box lets you change or edit the text on the Security Banner. You can also choose to not display the Security Banner once the Network Management Console applet is loaded.

To set the Security Banner text parameters:

1. Click the **Security Banner** tab at the top of the Options dialog box.
2. Do one of the following tasks:
   - To add a new text on the Security Banner:
     i. Select the existing text and delete the entire content.
     ii. Enter the new text.

iii. Click **Apply** to save the changes.

- To edit the existing text on the Security Banner:

  i. Click inside the existing text and make the changes.

  ii. Click **Apply** to save the changes.

- To revert back to the last saved text while editing the existing text on the Security Banner:

  Click **Reset**. The system displays the last saved text.

- To choose not to display the Security Banner:

  i. Clear **Show at startup** if you do not want the Security Banner to be displayed when the Network Management Console applet is launched.

  ii. Click **Apply** to save the changes.

Result

Note:

You should have write permissions to edit the text on the Security Banner.

For information on requesting write permissions, refer to Requesting write permission on page 34 and for information on how to set Read/Write default parameters, refer to Setting Read/Write defaults on page 41.

Setting Syslog server parameters

Now with the Network Management, you can choose to log important events and activities performed within the Enterprise Network to a Syslog host (a server or machine that receives syslog messages). This enables a centralized logging location where multiple instances of the Network Management can log their activities.

The Syslog Server tab of the Avaya Network Management Console's Options dialog box lets you configure the syslog servers to which logs are logged. You can configure one or multiple syslog hosts.

To set Syslog Server parameters:

1. Click the **Syslog Server** tab at the top of the options dialog box. The system displays the Syslog Server table.
2. Choose one of the following options.

   - To add new Syslog Server parameter:

i. Click **Add** to open a new row in the default table.
ii. Enter the Syslog server name in the **Server Name** field.
iii. Select the check box to enable logging to the Syslog Server.
iv. Enter the IP address of the Syslog server in the **IP Address** field.
v. Click **Apply** to add the new Syslog server configuration to the default table.

- To edit entries in the default table:
  i. Click the field you want to edit.
  ii. Edit the information in the field.
  iii. Click **Apply** to save the changes in the table.
- To delete a set parameter from the default table:
  i. Select a row or a range.
  ii. Click **Delete**.
  iii. Click **Apply** to delete the row or range from the default table.
- To revert back applied changes:
  i. Select the row you recently added or modified.
  ii. Click **Undo**.

Status of the row in the Avaya Network Management Console table

The Avaya Network Management Console informs you of the status of each row in a table. The following table shows symbols that appear at the start of a row, with their corresponding explanations.

Name	Description
	The row is a new entry.
	The row is to be deleted.
	The row has been modified.

Accessing Avaya Network Management Console help

This section explains how to use the on-line help in AvayaNetwork Management Console. The on-line help can be opened to the contents page or directly to a topic of interest.

To access the help, do one of the following:

- To open the help to the contents page, select **Help** > **Contents**. The online help opens to the contents page
- To open the help directly to a topic of interest:

  i. Do one of the following:

     1. Click  .
     2. Select **Help** > **Help On**. The cursor changes to the shape of an arrow with a question mark.

  ii. Click a point of interest in the AvayaNetwork Management Console. The help opens to a topic explaining the clicked feature.

Result

Note:

Web Help in Device Manager Application is available only for G430 Device Manager. All of the other Device Managers (G250/G350/G450/C360/P330) continue to use the Java Help.

Chapter 5: Avaya Network Management Console Network Tree

Network tree overview

When viewing the network, you may want to view:

- The structure of the network by subnet.
- The information categorized by the different types of devices in the network.
- The VoIP system view, which includes the voice elements in a data network, and the relationships between VoIP registered endpoints, gatekeepers, and call managers.

The Avaya Network Management Console's user interface provides an integrated view of the structure of the network, along with details about specific elements.

In addition, you may want to categorize the devices in your network by other criteria, such as workgroups or location. The AvayaNetwork Management Console allows you to create user defined views of your network and assign devices to custom categories. You can create up to five custom views of your network.

The left side of the user interface is the Network Tree. This provides a hierarchical view of the network. The right side of the user interface contains the Network table. Together, these views provide details about specific elements in the network.

When an element in the tree is selected, the elements immediately below the selected element appear in the Network table. Elements in the Network table are accompanied by fields providing details about the elements.

Viewing the network tree

There are two default views of the Network Tree - the Subnet View and the Device Type View. A third view, the VoIP System View, appears for networks containing VoIP devices. In addition, you can define up to five custom views of the network. The Subnet View shows a hierarchical representation of the subnets in the network. The Device Type View shows a view of the network grouped by device type. The VoIP System View shows a hierarchical representation of the voice devices in the network. To switch to a different view, click the appropriate tab above the tree.

To expand or contract the view of an element in the tree, do one of the following:

- Double-click the element.
- Click the handle next to the element you want to expand or contract.

Related topics:

Subnet view on page 50
Device type view on page 50
VoIP system view on page 51
Custom Views on page 53

Subnet view

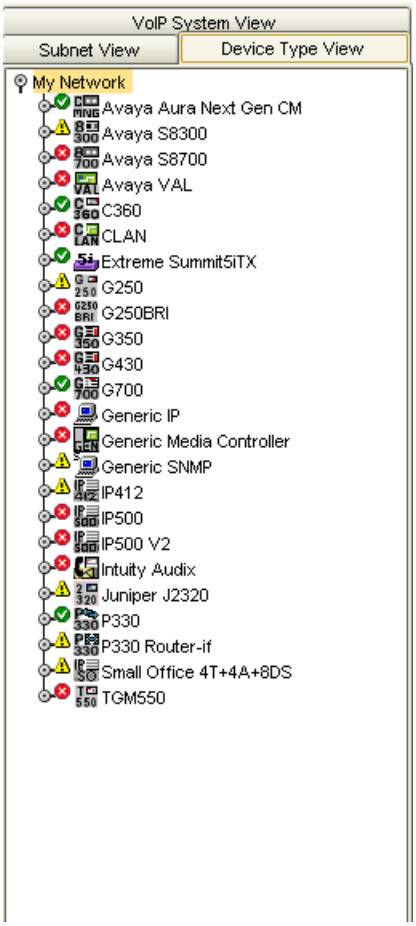
The Subnet view tree shows a hierarchical view of the subnets in the network. The Subnet view of the network contains the following levels:

- **My Network** — Represents the entire network tree. When selected, all subnets appear in the Network table.
- **Subnets** — Represents the subnets in the network. When selected, all devices with IP addresses in the selected subnet appear in the Network table.
- **Devices** — Each device is labeled with the logical name or IP address of the device. When a device is selected, the device's interfaces appear in the Network table.

Device type view

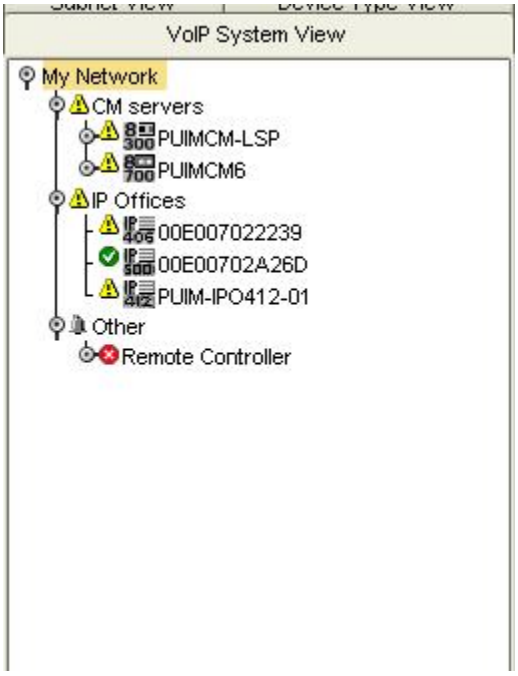
The Device Type View tree shows the network grouped by device type. The Device Type View of the network contains the following levels:

- **My Network** — Represents the entire network tree. When selected, all supported device types in the network appear in the Network table.
- **Device Types** — Represents all supported device types that appear in the network. When selected, all devices of the selected type appear in the Network table.
- **Devices** — Represents the devices in the network. When selected, the device's interfaces appear in the Network table.



VoIP system view

The VoIP System View tree shows a hierarchical view of the voice devices in the network. The VoIP System View tree is updated every time you run Discovery.



The root of the VoIP System View tree is **My Network**. It represents all voice devices in the network. The root splits into several branches including **SES Servers** (SIP Enablement Services Servers), and **CM Servers** (Avaya Aura® Communication Manager Servers), **Integral 55 Servers**, **IP Office** and **Other**.

The **SES Servers** branch splits based on the SIP Enablement Services Servers. Each discovered SES Server displays its own branch. Clicking an SES Server branch displays all discovered SIP series IP phones associated with the SES Server.

Under the **CM Servers** branch, the tree splits into various Avaya Aura®Communication Manager Servers. For each Communication Manager server, the CLANs, media gateways, voice adjuncts (example, Intuity Audix) appear based on the configuration.

For duplex S87xx Communication Manager Media Servers, the tree displays the Virtual server. Under the virtual server, the active server and the standby server are listed. For simplex servers, including the S85xx, S84xx, S83xx, and simplex S87xxs, only the active server is listed.

At this level, the tree also displays the following devices:

- CLANs - Displays the CLANs related to the Communication Manager. For each CLAN, all related Media Gateways (MGs) are listed under the MG branch. When you click a CLAN, all IP phones associated with the CLAN are displayed in the Registered Endpoints Table.
- VAL boards - Displays the VAL Boards related to the Communication Manager.
- Port Networks (PNs) - Displays the PNs that are controlled by the Communication Manager. Carriers that are part of the selected PN are listed under that PN.

- Enterprise Survivability Servers (ESSs) - Displays the ESSs for the Communication Manager. If the ESS controls some of the PNs in the tree (because they lost connectivity with the Communication Manager), these PNs appear directly under the ESS, rather than under the Communication Manager.
- Local Survivable Processors (LSPs) - Display the LSPs for the Communication Manager.
- Voice Adjuncts - Displays Voice Adjuncts for the Communication Manager.
- Media Gateways (MGs) - Only appear for Communication Managers, if the Communication Manager is running in processor ethernet mode. When you click an MG, all IP phones physically connected to the MG are displayed in the Port Connections Table.
- PNs - Displays the PNs that are controlled by the Communication Manager. Under each PN, the list of cabinets associated with the selected PN are displayed, showing the cabinet number and letter for each device.

The **IP Office** branch displays all IP Office devices. It supports the following types of devices:

IP406V2, IP412, IP500, IP500V2 (IP Office mode), Small Office 4T+4A+8DS, Small Office 2T +4A, and Small Office 4T+8A.

The **Other** branch splits into three. The **Unaffiliated** branch displays a list of MGs, whose affiliation with a Avaya Aura® Communication Manager media server cannot be determined. If you click an MG, IP phones physically connected to the MG are displayed in the Port Connections Table. The **Remote Controller** branch displays all MGs for which the controller could be found, but the controller's association with the Communication Manager could not be determined. The **ESS** branch displays a list of ESSs, whose affiliation with the Avaya Aura® Communication Manager media server cannot be determined.

Note:

To refresh the Port Connections or Endpoints table for connections or endpoints attached to a specific device, right click that device in the tree and select **Refresh Connections**.

Custom Views

The Network Management Console helps you create custom views of your network. This lets you design a view of your network based on criteria that are important to you. For example, you can design a custom view based on the location of devices or based on the functions that devices perform (that is, backbone switches, servers, important users, and so on.) This can help you focus on a particular set of devices.

Note:

Copy, Cut, and Paste functions are allowed in Custom Views only.

Related topics:

Creating Custom Views on page 54

Modifying Custom Views on page 54
Deleting Custom Views on page 55
Adding branches in Custom Views on page 55
Modifying branches in Custom Views on page 56
Deleting branches in Custom Views on page 56

Creating Custom Views

To create a custom view:

1. Select **File** > **New** > **View**. The system displays the New View dialog box.
2. Enter a name for the view in the **View Name** field.

   Note:
   View names cannot contain periods.
3. Enter a description of the view in the **Description** field.
4. Click **Apply** to add the view to theNetwork Management Console with the top level **My Network**. All devices in the network are added to a branch labeled **Unassigned**.

Modifying Custom Views

To modify a custom view:

1. Click the View Tab (refer to VoIP system view on page 51) associated with the custom view you want to modify.
2. Select **Edit** > **Modify View**. The system displays the Modify View dialog box.
3. Change the name for the view in the **View Name** field.

   Note:
   View names cannot contain periods.
4. Change the description of the view in the **Description** field.
5. Click **Apply** to modify the view.

Deleting Custom Views

To delete a custom view:

1. Click the View Tab (refer to VoIP system view on page 51) associated with the custom view you want to modify.
2. Select **Edit** > **Delete View**.
3. Click **Yes** on the confirmation dialog box to delete the custom view.

Adding branches in Custom Views

You can add branches to a custom view of the network and populate the branches with devices or nested branches.

To add branches to a custom view of the network:

1. Select the node in the Network Tree to which you want to add a branch.
2. Select **File** > **New** > **Branch**. The system displays the Add Branch dialog box.
3. Enter a name for the branch in the **Branch name** field.

   Note:
   Branch names cannot contain periods.
4. Enter a description of the branch in the **Branch Description** field.
5. Assign devices to the branch using the following procedure:
   - Select the devices you want to add to the branch in the **Unassigned** list and click  . The devices appear in the **Members** list.
   - Select the devices you want to remove from the branch in the **Members** list and click  . The selected devices are removed from the **Members** list.
6. Click **Apply** to add the branch and its devices to the selected part of the tree.

Modifying branches in Custom Views

You can add and remove devices from branches in a custom view of the network. To modify a branch of a custom view of the network:

1. Select the branch you want to modify in the Network Tree.

   Note:
   You cannot modify an **Unassigned** branch.
2. Select **Edit** > **Modify**. The system displays the Modify Branch dialog box.
3. Change the name of the branch using the **Branch name** field.

   Note:
   Branch names cannot contain periods.
4. Change the comment attached to the view in the **Branch Description** field.
5. Assign devices to the branch using the following procedure:
   - Select the devices you want to add to the branch in the **Unassigned** list and click . The devices appear in the **Members** list.
   - Select the devices you want to remove from the branch in the **Members** list and click . The selected devices are removed from the **Members** list.
6. Click **Apply** to modify the branch.

Deleting branches in Custom Views

You can delete branches from a custom view of the network.

To delete a branch from the custom view:

1. Select the branch you want to delete in the Network Tree.

Note:
You cannot delete the Unassigned branch.

2. Select **Edit** > **Delete**.
3. Click **Yes** on the confirmation dialog box to delete the branch, and displays all its devices in the Unassigned list.

Printing the Network Tree

You can perform the following tasks:

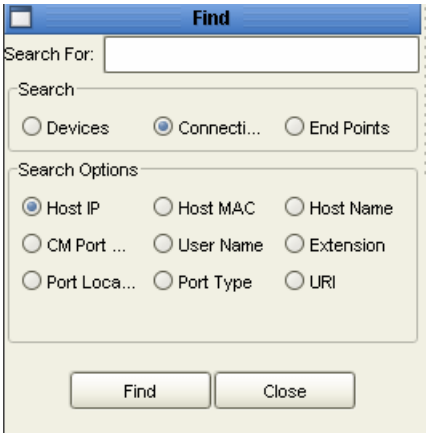
1. To print the current view of the Network Map, select **FIle** > **Print**. The current view of the Network Map is printed.
2. To view a preview of the printed Network Map, select **File** > **Print Preview**. The system displays the preview of the Network Tree.
3. To print the Network Map, click **Print**.
4. To close the Preview window without printing the map, click **Close**.

Searching the Tree

The Avaya Network Management Console lets you search the Network Map for specific elements.

To search the Network Map:

1. Do one of the following:
   a. Click  .
   b. Select **Edit** > **Find**. The system displays the Find dialog box.



2. Select **Devices**, **Connections**, or **End Points** under the **Search** area of the Find dialog box.
3. Select one of the options under the **Search Options** area of the **Find** dialog box.
4. Enter the device's name (or part of it), IP address, or MAC address in the **Search For** field.
5. Click **Find** to display the element you searched highlighted in the tree.
6. Do one of the following:
7. To find the next element that matches the search criteria, click **Find Next**. The element you searched for appears highlighted in the tree.
8. Click **Close**.

Chapter 6: Launching Applications

This chapter provides instructions for launching device specific applications and network wide applications from the Network Management Console.

For information specific to an application, refer to the application's User Guide or on-line help.

Device applications that can be launched from Network Management Console

Launching G860/Audio Codes Mediant 3000 EMS Client

If you need to launch the G860 EMS Client through **NMC** > **Tools**, do the following:

1. Manually add the following new System variable in Windows My Computer / System Properties / Advanced / Environmental Variables. ...Variable name: AUDIOCODES_DIR Variable value (without a back slash at the end): "C:\Program Files\AudioCodes\EMS Client 5.8.80".

   The exact EMS folder path will vary depending on which version of EMS client is installed on the user machine or which particular EMS Client version you want to launch through **NMC** > **Tools** if there are multiple EMS client versions on the user machine.
2. Restart Avaya services.
3. Log on to Network Management Console and select **Tools** > **G860 EMS Client**. This launches the GUI for G860/Audio Codes Mediant 3000 EMS Client.
4. Provide the login details for the EMS Client separately.

Related topics:

Supported G860 / Audio Codes Devices on page 60

Supported G860 / Audio Codes Devices

Network Management Console supports the following G860 Variants:

- G860 Mediant 5000
- G860 Mediant 8000
- Mediant 3000 (M3K)

Launching Device Manager

To launch the Device Manager for a managed device in the current Network Map:

1. Select the device.
2. Do one of the following:
   - Click  .
   - Select **Tools** > **Avaya Device Manager**.
   - Double-click the device. The system displays the Device Manager for the selected device.
   - Right-click the device and select **Device Manager** from the menu that appears.

Note:
When running a remote session of the Avaya Network Management Console, Device Manager can only be launched for devices that can be managed remotely.

Launching IP Office Manager

IP Office Manager is the device manager for the IP Office devices. It enables you to view and edit an IP Office device's configuration.

To launch the IP Office Manager:

1. Select the device you want to view in the Network Tree.
2. Double-click on the IP Office device.
   Network Management Console will launch the IP Office Manager.

Note:

IP Office Manager requires a login ID. Ensure the IP Office device has been assigned to an IP Office user in Secure Access Administration before launching IP Office Manager.

Launching IP Office System Status

IP Office System Status enables you to log into the selected IP Office system automatically without re-entering your login and password.

To launch IP Office System Status:

Select **Tools** > **IP Office System Status**.

Launching Telnet

Telnet can be used to access the Command Line Interface (CLI) of a network device. This allows you to change the device's setup. If you are running the Network Management remotely, you can use Telnet to manage devices whose Device Managers cannot be run remotely.

To launch a Telnet session to a managed device in the current Network Map:

1. Select the device.
2. Do one of the following:
   - Click  .
   - Select **Tools** > **Telnet**. A Telnet session opens to the device.
   - Right-click the device and select **Telnet** from the menu that appears.

Launching Web Session

Web Sessions can be used to manage devices that support Web Sessions over the Internet. These devices include some Avaya devices. In addition, non-Avaya devices that support Web

Sessions can be managed from both local and remote sessions of the Avaya Network Management.

To launch a Web Session, do one of the following:

- Select **Tools** > **Web**. A Web Session opens to the device.
- Right-click the device and select **Web Session** from the menu that appears.
- Select a device that supports Web Sessions, and then click  .

Pinging a device

The PING application lets you PING devices from within the Avaya Network Management Console. If you are having a problem communicating with the device via SNMP, try to ping the device. This helps you to determine whether the cause of the problem is related to the device's SNMP parameters or to a general communication problem with the device.

To PING a managed device:

1. Select the device.
2. Do one of the following:
   a. Select **Tools** > **Ping**. The results of the PING appear in the Command window.
   b. Right-click the device and select **Ping** from the menu that appears.

Launching an SSH session

Prerequisites

You can connect to a device using an SSH session. To launch an SSH session, you need to set the path to the SSH client application in the Configuration Utility tool. This is a one-time activity. You do not have to repeat this procedure each time you want to connect to a device using SSH. To set the path:

1. In the Network Management server, select **Start** > **Programs** > **Avaya** > **Tools** > **Configure Integrated Management.** The system displays the Configure Utility dialog box.
2. Click the **AIM Information** tab.
3. In the **Path to SSH client application** field, enter the directory path where you have installed the SSH client application.

   For example, if you have installed the SSH client in `C:\Program Files\SSH`, and the application (.exe) file is inside the SSH folder, enter `C:\Program Files\SSH\SSH.exe` in **Path to SSH client application** field.

To launch an SSH session:

1. Select the device.
2. Do one of the following:
   a. Select **Tools** > **SSH**.
   b. Right-click the device, and then select **SSH**.

Launching Avaya Site Administration

The Site Administration is a system management tool designed for user administration and maintenance of IP enabled Avaya Aura® Communication Manager telephony systems and IP phones. The Site Administration also provides terminal emulation capabilities for general administration of other types of voice devices.

Note:
The Site Administration is part of Avaya Integrated Management.

The Avaya Network Management Console recognizes Media Servers and IP phones that can be managed by the Site Administration. If you have the Site Administration installed on your computer, you can launch the Site Administration to manage an appropriate device from the Avaya Network Management Console.

To launch the main Site Administration window, select **Tools** > **Voice Applications** > **Avaya Site Administration** with no telephony device selected. The system displays the main Site Administration window.

To launch the Site Administration on an appropriate switch, gateway, or IP phone:

1. Select an appropriate managed telephony device.
2. Do one of the following: .
   - Select **Tools** > **Voice Applications** > **Avaya Site Administration**
   - Double-click an appropriate managed telephony device.
     - If you select a Communication Manager Media Server, the Site Administration connects to the device and opens the appropriate form for the server.
     - If you select an IP phone, theSite Administration connects to the Communication Manager Media Server controlling the selected phone and opens the appropriate form for the phone's extension.

Launching Avaya MultiSite Administration

The Avaya MultiSite Administration is a system management tool designed for configuration of the Avaya Aura® Communication Manager Media Servers and Media Gateways, and upgraded DEFINITY® servers.

Note:
The Avaya MultiSite Administration is part of Avaya Integrated Management.

To launch the main Avaya MultiSite Administration window:

Select **Tools** > **Voice Applications** > **Avaya MultiSite Administration** with no device selected. The system displays the main Avaya MultiSite Administration window.

To launch the Avaya MultiSite Administration on an appropriate device:

1. Select an appropriate managed device.
2. Select **Tools** > **Voice Applications** > **Avaya MultiSite Administration** .
   The Avaya MultiSite Administration opens on the selected device.

Launching Avaya Fault and Performance Manager

The Avaya Fault and Performance Manager is a system management tool designed for monitoring the performance and viewing faults on theAvaya Media Servers and Gateways, and upgraded DEFINITY® servers.

Note:

TheAvaya Fault and Performance Manager is part of Avaya Integrated Management.

To launch the main Avaya Fault and Performance Manager window, select **Tools** > **Voice Applications** > **Avaya Fault and Performance Manager** with no device selected. The system displays the main Avaya Fault and Performance Manager window.

To launch the Avaya Fault and Performance Manager on an appropriate device:

1. Select an appropriate managed device.
2. Select **Tools** > **Voice Applications** > **Avaya Fault and Performance Manager**.

   The Avaya Fault and Performance Manager opens on the selected device.

Launching Avaya Voice Announcement Manager

The Avaya Voice Announcement Manager is a system management tool designed for Voice Announcements over LAN (VAL) on Avaya switches that support VAL.

Note:

The Avaya Voice Announcement Manager is part of AvayaIntegrated Management.

To launch the main Avaya Voice Announcement Manager window, select **Tools** > **Voice Applications** > **Avaya Voice Announcement Manager** with no device selected. The system displays the main Avaya Voice Announcement Manager window.

To launch the Avaya Voice Announcement Manager on an appropriate Voice Announcement board:

1. Select an appropriate Voice Announcement board.
2. Do one of the following:
   a. Select **Tools** > **Voice Applications** > **Avaya Voice Announcement Manager**

b. Double-click an appropriate managed device. The Avaya Voice Announcement Manager opens on the selected device.

Launching Polycom GMS

The Network Management Console supports Polycom GMS for managing Polycom video conferencing gateways connected to your network.

To launch:

1. Select a supported Polycom gateway.
2. Do one of the following:
   - Select **Tools** > **Polycom GMS**. The system displays the Server-based Polycom GMS application.
   - Double-click a supported Polycom gateway. The embedded Web interface of Polycom GMS opens for the selected gateway.

Related topics:

Supported Polycom gateways on page 66

Supported Polycom gateways

The following Polycom gateways are supported:

- VSX 3000
- VSX 7000
- MGC 100
- MGC 100 Plus
- MGC 25
- MGC 25 Plus
- MGC 50
- MGC 50 Plus
- RMX 200

Launching network-wide applications

To launch a network-wide application:

1. Select **Tools** > ***Application Name*** , where *Application Name* is the name of the network-wide application you want to run. The network-wide application opens.

   Note:
   Not all network-wide applications can be launched when running a remote session of the Avaya Network Management Console.

Related topics:

Supported network-wide applications on page 67

Supported network-wide applications

The following network-wide applications are supported:

- Avaya Provisioning and Installation Manager for Gateways
- Avaya Provisioning and Installation Manager for IP Office Devices
- Avaya Software Update Manager
- Avaya Configuration Backup Restore
- Avaya SMON Manager
- Avaya easy Management
- Avaya NM Backup Utility
- G860/Audio Codes Mediant 3000 EMS Client

Chapter 7: Avaya Network Management Console Tables

This chapter provides a detailed description of the Network Table and Connections Table.

Network table

The Network table provides information about the objects in the selected branch of the Network Tree. The information in the Network table varies depending on the element selected in the Network Tree. The following sections provide an explanation of the fields and the color of devices in the Network table.

Related topics:

Network table fields on page 69
Network table colors on page 71

Network table fields

The following table lists the columns in the Network Table when the root of the Network Tree is selected in Subnet View.

Name	Description
Interface Status	The status of the device with the highest severity level in the subnet.
Name	IP address of the subnet.
No. of Devices	The number of devices that have an interface in this subnet.

The following table lists the columns in the Network Table when the root of the Network Tree is selected in Device Type View.

Name	Description
Interface Status	The status of the device with the highest severity level in the group of devices for the same device type.
Name	The device type.
No. of Devices	The number of devices from this type.

The following table lists the columns in the Network Table when a subnet or device type is selected in the Network Tree.

Name	Description
Interface Status	The status of the device.
Name	The Best Name of the device known to the Avaya Network Management Console.
IP address	The IP address of the device.
Subnet Mask	The subnet mask of the device's IP address.
Phone Extension	The phone extension of the device.
Device Type	The device type.
Read Community	The Read Community of the device.
Write Community	The Write Community of the device.
Retries	The number of times an application will poll a device without receiving a response before timing out.
Timeout	The number of seconds an application will poll a device without receiving a response before timing out (in milliseconds).

The following table lists the columns in the Network Table when a device is selected in the Network Tree.

Name	Description
Interface Status	The status of the interface.
IP Address	The IP address of the interface.
MAC Address	The MAC address of the device.
Subnet Mask	The subnet mask of the device's IP address.
Interface Number	The number of the interface.
Read Community	The Read Community of the device.
Write Community	The Write Community of the device.
Retries	The number of times an application will poll a device without receiving a response before timing out.
Timeout	The number of seconds an application will poll a device without receiving a response before timing out (in milliseconds).

Network table colors

Devices and interfaces viewed in the Network table are colored based on their status. The following table provides a list of colors and the statuses they represent.

Name	Description
Green	The device/interface/agent status is Okay. In case of a Avaya Aura® Communication Manager SNMP Agent, no alarms are present.
Yellow	The device/agent status is Warning. When it is a Avaya Aura® Communication Manager SNMP Agent, there are one or more minor/warning alarms present in the system.
Red	The device/interface/agent status is Fatal. When it is a Avaya Aura® Communication Manager SNMP Agent, there are one or more major alarms present in the system.
Off-White	The device is unmanaged.
Blue	The agent interface does not respond to SNMP. (Probably caused by an incorrect read community.)

The following diagram outlines the method used by the Network Management to determine the color of a device in the Network Table.

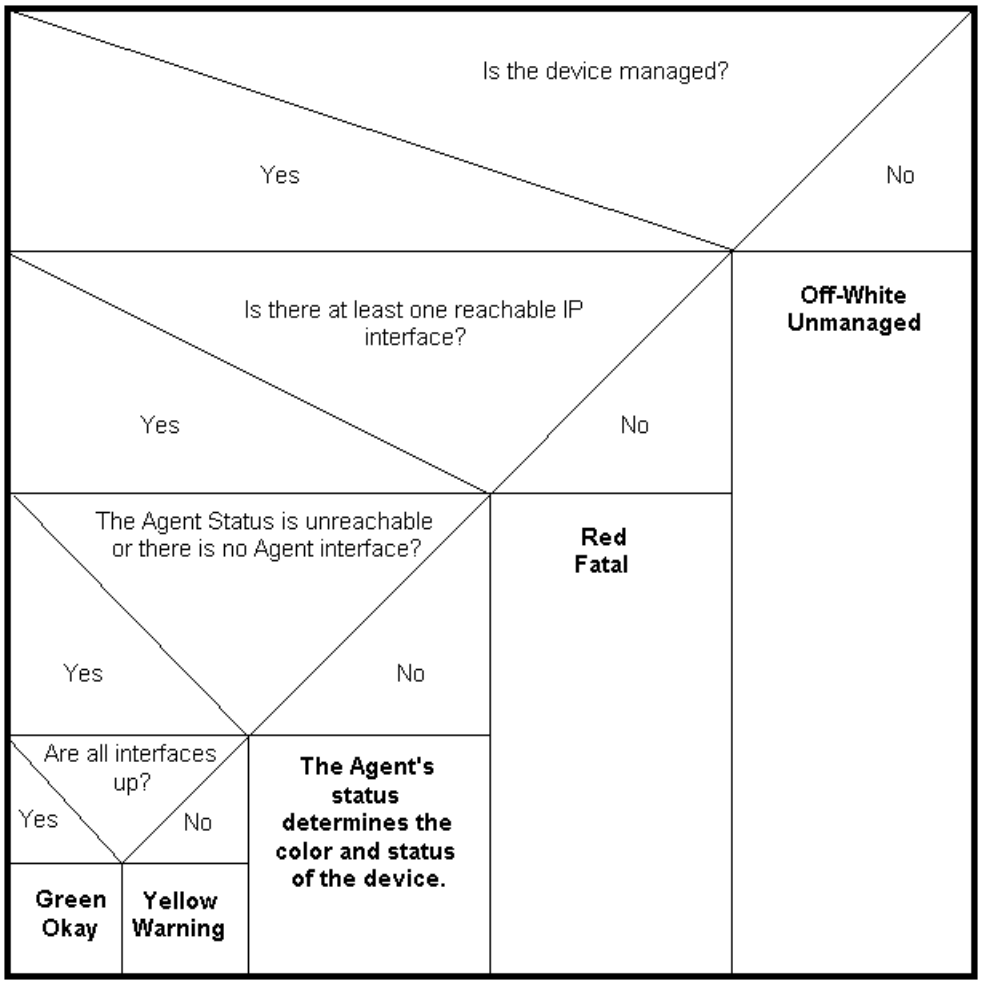


Table toolbar buttons

The table toolbar and search functions are common to the Network table and Dialog area of the Network Management Console. This area includes the Alarms table, Modules table, Interfaces table, Registered Endpoints table, and the Port Connections table.

The table below describes the toolbar buttons for the Alarms, Modules and Interfaces tables and the Port Connections/Registered Endpoints Tables:

Name	Description
	Saves the table to a .csv file.
	Opens the Select Columns list, which lets you select the columns you want to view in the table.

Name	Description
	Scrolls back through the pages in the table, when there are multiple pages of data. There is a maximum of 1000 entries per page.
	Scrolls forward through the pages in the table, when there are multiple pages. There is a maximum of 1000 entries per page.
	Opens the filter function, which lets you enter criteria for which to search in the table.
	Applies filter criteria specified in the filter row.

Related topics:

Choosing table parameters to display on page 73
Filtering the tables on page 73

Choosing table parameters to display

You can choose which parameters to display in a table.

To select the parameters you wish to view:

1. Click  . The system displays a list of available parameters.
2. Select the parameters that you wish to display in the table. The display is updated automatically as soon as the column is selected.

Filtering the tables

You can filter the information displayed in a table to display only the criteria you want to include.

To filter:

1. Select the view in which you want to work or the information that you want to display in the relevant table.
2. Click the **Turn on Filtering** button. A new row appears in the table, highlighted in blue.

3. In the new row, enter the filter criteria in the column you want to search. You can enter information in more than one field to narrow your search.
4. Click the **Filter** button to apply changes.

Alarms table

The Alarms Table displays all alarms raised for the devices in the Network Tree. The Alarms Table lets you see the status of AM110/ i40TS/ i120TS devices listed in the tree and any problems associated with them.The Network Management Console queries the network for alarm updates every 30 minutes and displays the results in the Alarms Table. A unique identifier and the severity level of the alarm are displayed for each alarm.

If a trap is received by the Network Management server, the Network Management Console immediately queries the device that sent the trap. The Alarms Table is updated immediately, regardless of the time elapsed since the last query was performed.

To view the Alarms Table, click the **Alarms** tab in the Network Table. Double-click an alarm to open the Event Manager focused on the alarm definition. The alarm description can be customized in the event manager in the same way that a trap description can be edited. To customize the alarm description, refer to Event Configuration window on page 121.

You can filter the alarms table by category, severity level, or description. For more information on filtering the alarms table and the alarms table toolbar, refer to Table toolbar buttons on page 72.

Related topics:

Alarms table parameters on page 74

Alarms table parameters

The following table lists the fields that can be found in the Alarms Table:

Name	Description
Severity	An icon representing the severity of the alarm: • - Info • - Warning • - Minor

Name	Description
	• - Major • - Critical
Category	The category of the alarm.
Start Time	The time the alarm was reported.
Description	A description of the alarm.

Modules table

The Modules table displays the modules associated with the gateways listed in the Network Tree. For information on viewing the Modules table and the Modules table toolbar, refer to Table toolbar buttons on page 72.

Related topics:

Modules table parameters on page 75

Modules table parameters

The following table lists the fields that can be found in the Modules table:

Name	Description
Module Index	Location of the module inside the box.
Module Type	Type of module.
Description	Description of the module.

Managing Objects

The Network Map includes all devices that have been discovered. You can control which of these devices are managed (monitored by theAvaya Network Management Server) and which of these devices are unmanaged (not monitored by the Avaya Network Management Server). If there are many objects in your Network Map, managing all of the objects may put stress on your network resources. You may also want to keep devices that do not need management, such as workstations, in the Network Map.

When an object in the Network Map is unmanaged, you cannot communicate with the device using the Avaya Network Management Console, and the device's color in the Network Table

is off-white. In addition, the Network Management does not test the device's connectivity status (PING) or receive any traps from an unmanaged device.

You can perform the following tasks on objects.

1. To unmanage an object:
   a. Select the object in the Network Table.
   b. Select **Edit** > **Unmanaged object** to unmanage the selected object.
2. To manage an unmanaged object:
   a. Select the object in the Network Table.
   b. Select **Edit** > **Manage object** to manage the selected object.

Manually adding devices

You can manually add devices to the Network Map. To manually add a device to the current Network Map:

1. Select **File** > **New** > **Device**. The system displays the Add Device dialog box to the **Basic Information** tab.
2. Enter the device's parameters in the Add Device dialog box.
3. To edit the device's SNMP parameters, click the **SNMP Access** tab.
4. Enter the SNMP parameters.
5. Click **Apply** to add the device to the Network Map.

Result

For information on the fields in the Add Device dialog box, refer to Device parameters on page 77.

Modifying devices

To modify basic information or SNMP parameters for a device in the current Network map:

1. Select a device.
2. Select **Edit** > **Modify**. The system displays the Modify Device dialog box with the selected device's parameters.
3. Modify the parameters in the Modify Device dialog box.

   Note:
   For information on the fields in the Modify Device dialog box, refer to Device parameters on page 77.
4. To edit the device's SNMP parameters, click the **SNMP Access** tab.
5. Modify the SNMP parameters.
6. Click **Apply** to modify the parameters.

Device parameters

The following table provides a list of the parameters in the Add Device and Modify Device dialog boxes.

Name	Description
IP Address	IP address of the device.
Mask	The IP subnet mask.
MAC	The MAC address of the agent.
Device Name	The name or best name of the device.
Device Type	Type of device. Possible types are: • **Auto Discover** — Avaya Network Management Server polls the device to determine the device type. • **Avaya Device** — Where Avaya device is the name of an device. • **Generic SNMP** — For other SNMP Devices. • **Generic IP** — For IP Devices that do not use SNMP. • **Other Device** — Where Other Device is another recognized device type.

Name	Description
Status	The managed status of the device. Possible statuses are: • **Manage** — The device is managed by Network Management. • **Un-manage** — The device is not managed by Network Management.
SNMP	The SNMP protocol. Possible SNMP protocols are: • **Snmp V1** • **Snmp V3**
Read Community	The device's read community. Only applicable for SNMP protocol V1.
Write Community	The device's write community. Only applicable for SNMP protocol V1.
User	A user name as defined in the Avaya Secure Access Administration application. Only applicable for SNMP protocol V3.
Retries	The number of times an application polls a device without receiving a response before timing out.
Timeouts (milliseconds)	The number of milliseconds an application polls a device without receiving a response before timing out.

Deleting devices

To delete a device from the Network map:

1. Select a device. To select more than one device, press `Ctrl` while selecting additional devices.
2. Select **Edit** > **Delete object**.
3. Click **Yes** on the confirmation dialog box to delete the selected device from the Network map.

Opening the Port Connections table

The Port Connections table provides information about ports on a selected device and the host devices connected to those ports. This information helps you understand the details of network topology, and keep track of inventory for devices such as IP phones.

To open the Port Connections table:

1. Open the Find dialog box (refer to Searching the Tree on page 57).
2. In the **Search** area, select **Connections**.
3. In the **Search Options** area, select the desired option to target a device.
4. Click **Find**. The system displays the Port Connections/Registered Endpoints dialog box and displays the Port Connections table for the selected device.

Note:
You can also view the Port Connections table for a device by selecting that device and then clicking **View** > **Connections/Endpoints**.

Result

You can choose the parameters displayed in the Port Connections table and filter the results of your search. For more information on viewing and filtering the Port Connections table and a description of the Port Connections toolbar, refer to Table toolbar buttons on page 72.

Related topics:

Port Connections table parameters on page 79

Port Connections table parameters

The following are the fields in the Port Connections table and their descriptions:

Name	Description
Module	The module or slot number.
Port	The port name or number.
CM Port Address	The Communication Manager port address.
Port Description	The type of port.
User Name	The User Name for the selected phone.

Name	Description
Extension	The phone extension number. Available for connected phones only.
URI	The SIP URI. Available for connected phones only.
Vlan	The Vlan for devices supported by the port selected.
Model	The model of the phone connected to the selected device.
Host IP	The IP address of the connected host.
Host Name	The name of the connected IP host, if available. If the connection is a link to another switch, the name value is “Backbone”.
Host MAC	The MAC address of the connected host.

Opening the Registered Endpoints table

The Registered Endpoints table displays details about the phones controlled by the selected node in the tree.

To open the Registered Endpoints table:

1. Open the **Find** dialog box (refer to Searching the Tree on page 57).
2. In the **Search** area, select **Endpoints**.
3. In the **Search Options** area, select the desired option to target a device.
4. Click **Find**. The system displays the Port Connections/Registered Endpoints dialog box and displays the Registered Endpoints table for the selected device.

Result

You can choose the parameters displayed in the Registered Endpoints table and filter the results of your search. For more information on viewing and filtering the Registered Endpoints table and a description of the Registered Endpoints toolbar, refer to Table toolbar buttons on page 72.

Related topics:

Registered Endpoints table parameters on page 80

Registered Endpoints table parameters

The following are the fields in the Registered Endpoints table and their descriptions:

Name	Description
User Name	The User Name for the selected phone.
Extension	The phone extension number. Available for connected phones only.
URI	The SIP URI. Available for connected phones only.
Module	The module or slot number.
Port	The port name or number.
CM Port Address	The IP address of the Communication Manager port.
Port Description	The description of the port as provided by the Communication Manager.
Vlan	The Vlan for devices supported by the port selected.
Model	The type of phone connected to the selected device.
Host IP	The IP address of the connected host.
Host Name	The name of the connected IP host, if available. If the connection is a link to another switch, the name value is “Backbone”.
Host MAC	The MAC address of the connected host.

Opening the Inventory table

The Inventory table provides information for all ports/endpoints and their associated devices over multiple devices on the network. The Inventory filter enables you to search the Inventory table and to refine the information displayed.

To open the Inventory table:

Select **View** > **Inventory**. The system displays the Inventory table. Click the appropriate tab. The available tabs are, **Ports** and **Endpoints**.

Related topics:

Inventory table toolbar on page 82
Inventory table parameters on page 82
Filtering the inventory table on page 84
Choosing Inventory table parameters to display on page 84

Inventory table toolbar

The table below describes the buttons on the Inventory table.

Name	Description
	Saves the Inventory table to a `.csv` file.
	Opens the Select Columns list, which lets you select which columns to view in the Inventory Table.
	Scrolls back through the Inventory pages when there are multiple page entries. There is a maximum of 1000 entries per page.
	Scrolls forward through the Inventory pages when there are multiple page entries. There is a maximum of 1000 entries per page.
	Opens the filter function, which lets you enter criteria for which to search in the Inventory table.
	Applies filter criteria specified in the filter row. This button only appears on the toolbar after the filter button has been selected.

Inventory table parameters

The following are the fields in the Ports tab of the Inventory table and their descriptions:

Name	Description
Module	Select a specific module on the device for which to view connections, or view connections for all modules on the device. This parameter is displayed by default.
Port	The port where the connection resides. This parameter is displayed by default.
CM Port Address	The IP address of the Communication Manager port.
Port Description	The description of the port as provided by the Communication Manager.
Switch IP	The IP address associated with the port. This parameter is displayed by default.
User Name	The User Name for the selected phone. This parameter is displayed by default.
Extension	The extension number, for connected IP phones only. This parameter is displayed by default.
URI	The SIP URI. Available for connected phones only.

Name	Description
Vlan	The Vlan for devices supported by the port selected.
Model	The model of the phone connected to the selected device. This parameter is displayed by default.
Host IP	The IP address of the connected host. This parameter is displayed by default.
Host Name	The name of the connected host, if available. If the connection is a link to another switch, the name value is **Backbone**.
Host MAC	The MAC address of the connected host.

The following are the fields in the Endpoints tab of the Inventory Table and their descriptions.

Name	Description
Media Controller	The media controller for the selected endpoint.
User Name	The User Name for the selected phone. This parameter is displayed by default.
Extension	The extension number, for connected IP phones only. This parameter is displayed by default.
URI	The SIP URI. Available for connected phones only.
Module	Select a specific module on the device for which to view connections, or view connections for all modules on the device. This parameter is displayed by default.
Port	The port where the connection resides. This parameter is displayed by default.
CM Port Address	The IP address of the Communication Manager port.
Port Description	The description of the port as provided by the Communication Manager.
Vlan	The Vlan for devices supported by the port selected.
Model	The model of the phone connected to the selected device. This parameter is displayed by default.
Host IP	The IP address of the connected host. This parameter is displayed by default.
Host Name	The name of the connected host, if available. If the connection is a link to another switch, the name value is **Backbone**.
Host MAC	The MAC address of the connected host.

Filtering the inventory table

To filter the inventory table:

1. Click the **Turn On Filtering** button to display a new row in the Inventory table, highlighted in blue.
2. In the new row, enter the filter criteria in the column you want to search.

   Note:
   Search by substring only. You can enter more than one substring.
3. Click the **Filter** button to display search results.

Choosing Inventory table parameters to display

You can choose which parameters to display in the Inventory Table.

To select the parameters you wish to view:

1. Click  to display a list of available parameters.
2. Select the parameters that you wish to display in the Inventory Table. The display is updated automatically as soon as the column is selected.
3. Click  to hide the list of available parameters.

Chapter 8: Network Maps

Network maps overview

The Network Map is the set of devices that can be viewed in the Avaya Network Management Console. The database lets you store information on the devices found in a Network Map. You can create a number of Network Maps and save them in the database. This can be useful in maintaining backups when major changes are made to the Network Map. When changes are made to a Network Map, they are saved in the map's Postgres database.

Devices can be imported into a Network Map from a text file. In addition, you can export the Network Map for use with other applications. For more information on exporting the current Network Map, refer to Exporting the Network Map on page 88.

Creating a Network Map

To create a new Network Map:

1. Select **File** > **New** > **New Map**. The system displays the Create New Map dialog box.
2. Enter a name for the file in the **New map name** field.
3. Click **OK** to create a new Network Map.
4. Add subnets and devices to the Network Map using one of the following methods:
   - *Discovery* - For more information, refer to Discovery of subnets and nodes on page 108.
   - *Manual Entry* - For more information, refer to Manually adding devices on page 76.
   - *Importing* - For more information, refer to Importing devices into the Network Map on page 87.

Related topics:

Opening a Network Map on page 86

Saving a Network Map to a different name on page 86
Printing a Network Map on page 86
Deleting a Network Map on page 87

Opening a Network Map

To open a Network Map:

1. Select **File** > **Open map**. The system displays the Open Map dialog box.
2. Select a Network Map from the list.
3. Click **Open**. The system displays the selected Network Map.

Saving a Network Map to a different name

To save a Network map to a different name:

1. Select **FIle** > **Save map**. The system displays the Save Map As dialog box.
2. Enter a name for the file in the **Map name** field.
3. Click **Save As** to save the Network map.

Printing a Network Map

To print a Network map:

Select **File** > **Print**. The Network map is printed.

Deleting a Network Map

Note:
You cannot delete the default map from the Network Management Console.

To delete a Network map:

1. Select **File** > **Delete map**. The system displays the Delete Map message box.
2. Click **OK** after you close all the opened Network Management applications. The system displays the Delete Map dialog box with the list of available maps.
3. Select the map you want to delete.
4. Click **Delete**. The selected map is deleted and the system displays the default map in the Network Management Console.

Importing devices into the Network Map

Devices can be imported from a text file into the Network Map. The information for each device must be on a single line, with the various information fields for the device separated by commas. This file is referred to as a Comma Separated Value (CSV) file.

The following is an example of rows in a CSV file:

```
.1.3.6.1.4.1.23.1.6.4.11,149.49.32.253,149.49.48.215,255.255.255.0,00:C0:4F:91:1A:
26,D
ays2,Days2,30,5
.1.3.6.1.4.1.23.1.6.4.11,149.49.32.184,149.49.48.91,255.255.255.0,00:C0:3E:
11:B3:14,Ve
nus,,,45,6
.1.3.6.1.4.1.23.1.6.4.11,149.49.32.251,149.49.43.210,255.255.0.0,00:C0:1F:
01:C2:11,Laz
y23,Lazy23,20,3
,149.49.48.204,255.255.255.0,00:A7:F2:11:BA:34,Oddball,Harpo,Harpo,60,7
```

Note:
The information fields of the CSV file can be different depending on whether SNMP V1 or V3 is active.

For information on the structure of CSV files of devices to import to a Network Map, refer to CSV file structure on page 88.

To import devices from a CSV file into the current Network Map:

1. Select **File** > **Import map**.
2. Browse to the CSV file.
3. Click **Open**.
   The devices in the CSV file are imported into the current Network Map.

   If a device listed in the file has the same IP address as a device already existing in the Network Map, the device details in the CSV file overwrite those in the Network Map. If a syntax error exists in the CSV file, the import stops after it has processed all the devices listed before the error.

Exporting the Network Map

The current Network Map can be exported to a CSV file for use with external applications, such as Microsoft Excel. For information on the structure of CSV files of exported Network Maps, refer to CSV file structure on page 88.

To export a Network map:

1. Select **File** > **Export map**.
2. Browse to the directory to which you want to save the file.
3. Enter a name for the CSV file in the **Name** field.
4. Click **Save** to export the current Network Map to the specified CSV file.

Related topics:

CSV file structure on page 88

CSV file structure

The structure of the information in the CSV file is described in the following table.

Name	Description
Device Type SysOId	The SysOId that defines the type of device. **Note:** For IP Devices that do not use SNMP, this field is empty.

Name	Description
IP Address	The IP address of the device.
IP Subnet Mask	The IP subnet mask.
Agent MAC Address	The MAC address of the agent.
Name	The name or best name of the device.
Read Community	The read community of the device. Only applicable for SNMP protocol V1.
Write Community	The write community of the device. Only applicable for SNMP protocol V1.
Timeouts	The number of milliseconds an application polls the device without receiving a response before timing out.
Retries	The number of times an application polls the device without receiving a response before timing out.
User	A user name as defined in the Secure Access Administration application. Only applicable for SNMP protocol V3.

Chapter 9: Network Discovery Wizard

Network Discovery Wizard overview

The Network Discovery Wizard opens at the end of the Network Management offer installation process. The Network Discovery Wizard lets you configure the Avaya Aura® Communication Manager Media Servers and the Network Management Console to properly discover the network.

Opening the Network Discovery Wizard

To open the Network Discovery Wizard:

Select **Actions** > **Network Discovery Wizard** from the Network Management Console's **Action** menu.

Using the Network Discovery Wizard

This section provides detailed information on each of the screens within the Network Discovery Wizard. To continue to the next screen, click Next. To return to an earlier screen, click Back. To exit the Network Discovery Wizard without making any changes, close the wizard.

1. Select **Actions** > **Network Discovery Wizard** from the Network Management Console's **Action** menu. The system displays the Welcome Screen.

   The Network Discovery Wizard provides a simple, step-by-step method for configuring the Communication Manager servers and for properly discovering and

managing your voice network with the Network Management Console. The steps of this method are described on the Welcome Screen.

2. Click **Next**. The system displays the Configure CM Servers screen. Do one of the following:

   • To add a Communication Manager:

      i. Click **Add CM**.

      ii. In the **IP Address** field, enter the IP Address of the Communication Manager server.

      iii. In the **Login** field, enter the login name as configured on the Communication Manager server.

      iv. Specify whether the Communication Manager server uses a password or ASG Key for login, and enter the string in the **Password**, or **ASG Key** field.

      Note:
      The ASG key is a 20-character octal code, the 19th character of which must be either 0, 2, 4, or 6, and the 20th character of which must be 0.

      v. In the **Protocol** field, select the protocol for communication with theCommunication Manager server. The protocols available are: SSH and Telnet.

      Important:
      Avaya recommends SSH as a secure protocol and Telnet is disabled by default.

      Note:
      Before accessing the Communication Manager server using passwords, you must verify theCommunication Manager server certificate. To ensure that this is the Communication Manager server you want to manage, verify that the public key is identical to the public key of the Communication Manager server certificate.

   • To edit the parameters for an existing Communication Manager server:

      i. Select the Communication Manager server from the **CM Servers Table**.

      ii. Click **Edit CM**.

   • To delete an existing Communication Manager server:

      i. Select the Communication Manager from the **CM Servers Table**.

      ii. Click **Remove CM**.

3. Click **Next**. The Network Discovery Wizard lets you select the SNMPv3 user that is used to communicate with the Communication Manager server. Do one of the following:
   - To use an existing SNMPv3 user:
     i. Select the **Existing SNMPv3 User** option.
     ii. Select the user from the **Select User** drop-down list.
   - To create a new SNMPv3 user with which to communicate with the Communication Manager:
     i. Select the **New SNMPv3 User** option.
     ii. In the **User Name** field, enter the user name for the new SNMPv3 user.
     iii. In the **Authentication Password** field, enter the SNMPv3 authentication password, and enter it again to verify the password in the **Verify Authentication Password** field.

     Note:
     The **Authentication Scheme** supported by theCommunication Manager is displayed. This field is read-only.
     iv. In the **Privacy Password** field, enter the SNMPv3 privacy password and enter it again to verify it in the **Verify Privacy Password** field.
4. Click **Next**. The Network Discovery Wizard lets you verify the Communication Manager server certificate. When you have finished reviewing the certificate, do one of the following:
   - Click **No**, to return to step 2.
   - Click **Yes**. The system displays the Configure global SNMP Parameters screen.
5. The Network Discovery Wizard lets you manage SNMP parameters used for network discovery and management access to the devices in your network.

   Note:
   These parameters can be modified later using the **FIle** > **Options** dialog box in the Network Management Console.

   Do one of the following:
   - To add an SNMP parameters set to the **SNMP Parameters Table**, Click **Add SNMP Rule**, and do one of the following:
     i. To edit the parameters for an existing SNMPv3 user:
        1. Select the **Existing SNMPv3 User** option.

2. Select the user from the **Select User** drop-down list.

ii. To add a new SNMPv3 user:

1. Select the **New SNMPv3 User** option.
2. In the **User Name** field, enter the user name for the new SNMPv3 user.
3. In the **Authentication Password** field, enter the SNMPv3 authentication password for the new user and enter it again to verify the password in the **Verify Authentication Password** field.

Note:
The **Authentication Scheme** supported by the Communication Manager is displayed. This field is read-only.

4. In the **Privacy Password** field, enter the SNMPv3 privacy password and enter it again to verify in the **Verify Privacy Password** field.

iii. To add an SNMPv1 community:

1. Select the **SNMPV1 Community** option.
2. In the **Read Community** field, enter the read community.
3. In the **Read/Write Community** field, enter the read/write community.

- To edit the parameters for an existing SNMP set:

i. Select the SNMP parameters set you want to edit from the **SNMP Parameters Table**.

ii. Click **Edit SNMP Rule**.

- To remove an existing SNMP parameters set:

i. Select the SNMP parameters set from the **SNMP Parameters Table**.

ii. Click **Remove SNMP Rule**.

6. Click **Next**. The system displays the Configure Network Subnet to Discover screen. Do one of the following:

- To add a network to the **Subnets Table**:

i. Click **Add Subnet**.

ii. In the **Subnet IP** field, enter an IP address for the new subnet.

iii. Select whether you want to provide the **Subnet Mask** or **Router** for this subnet, and enter the Subnet Mask or Router IP address.

- To edit the parameters for an existing network:

  i. Select the IP of the network from the **Subnets Table**.

  ii. Click **Edit Subnet**. You can now edit the parameters.

- To remove an existing network:

  i. Select the IP of the network from the **Subnets Table**.

  ii. Click **Remove Subnet**. The selected IP of the network is removed from the **Subnets Table**.

7. Click **Next**. The system displays the Configuration complete screen. Do one of the following:

   - Click **Finish** to start the automatic network discovery process.
   - Click **Back** to make any changes to the parameters you chose in the previous steps. Once you make the changes, click **Next** until you reach the Configuration complete screen, and then click **Finish**.

Note:

After the discovery is complete, the computer reboots and the configuration is incorporated in the Network Management Console. You can modify all parameters later using theNetwork Management Console's **File** > **Options** dialog box.

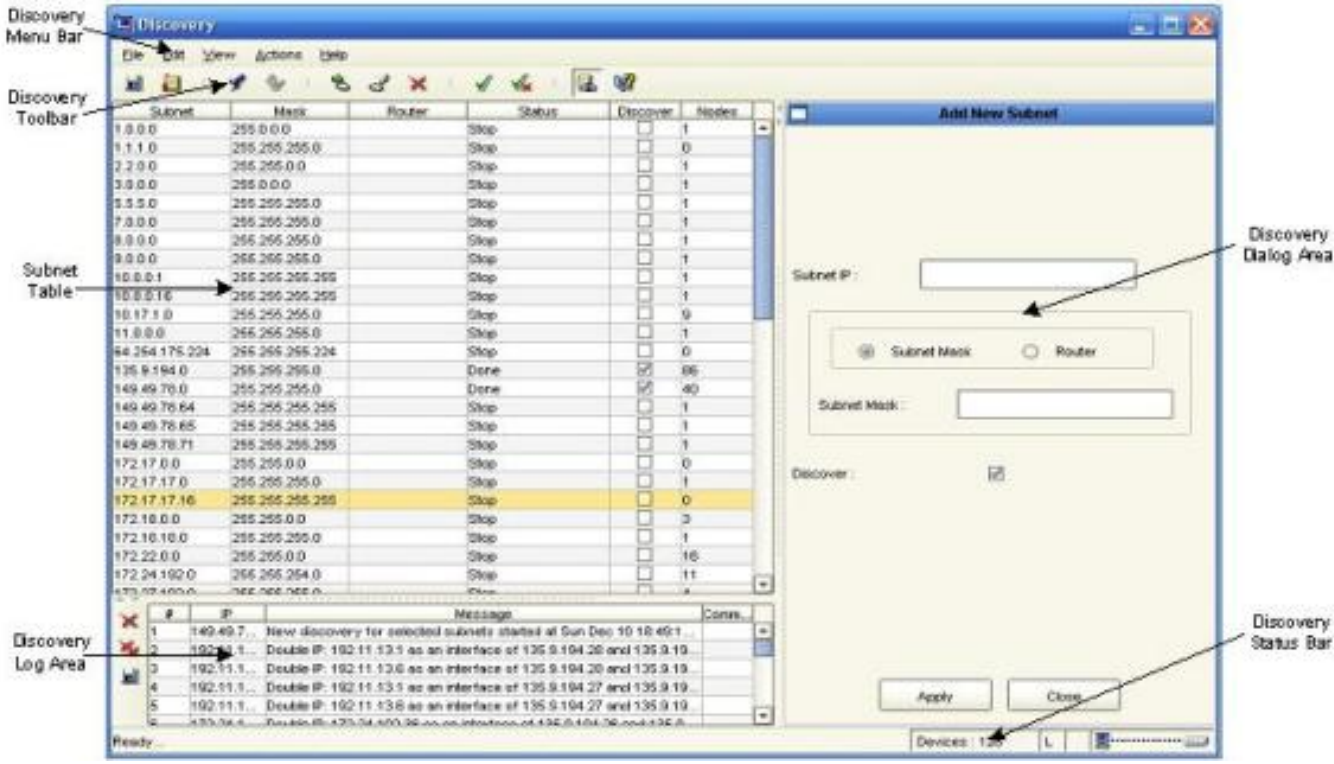
Chapter 10: Introduction to the Discovery window

Opening the Discovery window

To open the Discovery window, do one of the following:

- Click  .
- Select **Actions** > **IP Discovery**. The system displays the Discovery window.

Result



Discovery toolbar

The table below describes the buttons on the Discovery toolbar and gives the equivalent menu options.

Button	Description	Menu Item
	Saves the current Discovery settings.	**File** > **Save As**
		File > **Update Map**
	Opens the Discovery Options dialog box.	**File** > **Options**
	Starts a Discovery based on the default routers of the management station and the contents and settings of the Subnet table.	**Actions** > **Discover**
	Stops a Discovery process.	**Actions** > **Stop Network Discovery**
	Adds a subnet to the Subnet table.	**Edit** > **Add**
	Opens the Modify Subnet dialog box.	**Edit** > **Modify**
	Deletes the selected subnet from the Subnet table.	**Edit** > **Delete**
	Selects the **Discover** field for the selected subnet.	**Edit** > **Select**
	Clears the **Discover** field for the selected subnet.	**Edit** > **Unselect**
	Opens the Discovery log.	**View** > **Discovery Log**
	Opens context-sensitive help.	**Help** > **Help On**

Subnets table

The Subnets table contains a list of subnets from the following sources:

- The current Network Map.
- Subnets added to the Subnets table manually by the user.
- Subnets found in a Discovery.

The following table provides a list of the fields in the Subnets table and provides an explanation of each field.

Name	Description
Subnet	The IP address of the subnet.
Mask	The subnet mask.
Router	The IP address of the subnet's router.
Status	The status of Discovery on this subnet. Possible statuses are: • Stop — The Discovery was stopped by the user. • In progress — Discovery on this subnet is currently in progress. • Done — Discovery on this subnet has been completed.
Discover	A check box determining whether or not Discovery should search for nodes on the subnet. • Selected: Discovery can search for nodes on this subnet. • Cleared: Discovery cannot search for nodes on this subnet.
Nodes	The numbers of nodes discovered in the subnet.

To sort the Subnet table by one of the fields, click the field's column header. To reverse the sort order, click the column header again.

Discovery Dialog area

The area at the right of the Subnets table is where all dialog boxes open. This area can be resized by dragging the vertical splitter bar with the mouse. When a dialog box opens, it replaces the current dialog box open in the Dialog area. When no dialog box is open, the Dialog area disappears and the Subnets table expands to take its place.

Discovery log area

The area under the Subnets table is where the Discovery log opens. This area can be resized by dragging the horizontal splitter bar with the mouse. When the Discovery log is closed, the log area disappears and the Subnets table expands to take its place.

Discovery status bar

The Discovery status bar provides information about the current Discovery including:

- Current Discovery Phase — The phase of the current Discovery. Possible phases are:
    a. Ready — There is no Discovery in progress.
    b. Discovering Devices — Discovery is searching for subnets and routers.
- Devices — The total number of devices found in the current Discovery.
- Entries in the Log — If there are entries in the Discovery log, the letter “L” appears in the status bar. For information on viewing the Discovery log, refer to Using the Discovery log on page 113.
- Changes Found — If Discovery found subnets and/or nodes that are not in the current database, the letter “D” appears in the status bar.

Closing the Discovery window

To close the Discovery window:

Select **File** > **Exit**. The Discovery window closes.

Chapter 11: Discovering your network

This section provides detailed instructions on how to use the Avaya Network Management Console IP Discovery feature.

You can use the IP Discovery feature to discover all the supported nodes on your network. The system displays a list of subnets or an empty list when you run the IP Discovery for the first time.

There are two ways you can specify subnets to discover after selecting **Add** from the Edit menu or clicking the **Add** button on the toolbar:

- You can specify the Subnet IP address and the subnet mask.
- You can specify the Subnet IP address and a router interface which serves as the router for the given subnet. Upon discovery, the router is contacted and the subnet mask is determined using the standard interface SNMP query.

From Network Management Release 5.2 service pack 3 there is a new menu option in the Actions menu called **Discover Interfaces** and it is not selected by default.

When you select this option, you can query all SNMP-enabled devices for their IP interfaces and display them in the device list of Network Management Console. Also, the IP information of the directly connected subnets is automatically added to the subnet list of the discovery window, however they won't be checked for discovery by default.

If you do not select this option, you can discover only the primary management interface (PMI) of the supported device.

The discovery process sequence consists of the following steps:

1. IP Discovery
2. VoIP System View Discovery
3. IP Phone Data Discovery
4. Port Connection Discovery

Note:
From Network Management Release 5.2 service pack 3, Network Management Console does not use ICMP Echo messages (ping packets) for discovery. Discovery process is exclusively based on the SNMP protocol instead.

Note:
All toolbar buttons and menu items referred to in this section are in the Discovery window.

Understanding the IP Discovery process

The IP Discovery process is as follows:

1. Network Management Console queries the first subnet from the list. When the subnet definition is router-based, Network Management Console queries the specified router for its interfaces using the standard interface MIB query. Once the subnet mask is determined it continues with the discovery.

   Note:
   Make sure that the **Actions** > **Dicovery Interfaces** check box is selected in case of a router-based discovery.

2. Network Management Console retrieves the parameters of the first SNMP community string from the SNMP list.

   Note:
   The SNMP versions and community strings used during discovery are defined in Network Management Console's **File** > **Options** > **SNMP Access** page. Community strings are processed from the top to the bottom, so smaller the index, the sooner the SNMP community string will be tested during discovery.

3. Network Management Console sends a standard MIB query to each IP address in the given subnet for getting the “sysoid” value of the device using the community string parameters.
4. When SNMP timeout value expires and no reply is received to the query,Network Management Console attempts to send additional queries until the number of SNMP retries value expires. Otherwise Network Management Console proceeds with step 6.
5. When no SNMP response is received after both SNMP timeout and SNMP retries have expired, Network Management Console processes the next community string from the list and continues with step 3.
6. Network Management Console queries the “sysname” SNMP MIB value to get the system name.
7. If the **Actions** > **Dicovery Interfaces** check box is selected, Network Management Console will query the device for all of it’s IP interfaces using the IP-MIB. The interface list will be associated with the device and will be displayed in Network Management Console unless the interface IP address is excluded according to the list of excluded IP addresses. Also, whenNetwork Management Console detects that the interface connects a subnet that is not listed in the the subnet list of IP

Discovery, the subnet is automatically added to the list but it will not be checked for discovery by default.

8. Subsequent IP addresses and subnets are probed using the same method.

Setting Discovery options

The Discovery Options dialog box allows you to configure the Discovery options. Using the Discovery Options dialog box, you can configure the method and range of Discovery, the method Discovery uses for selecting names for discovered nodes, and the types of nodes Discovery can find.

To open the Options dialog box, do one of the following:

- Click  in the Discovery toolbar.
- Select **File** > **Options** in the Discovery menu bar. The system displays the Discovery Options dialog box.

Related topics:

Configuring Discovery method and range on page 103
Configuring the Discovery naming method on page 105
Selecting device types to discover on page 106

Configuring Discovery method and range

To configure the method and range of Discovery:

1. Do one of the following:
   - Click  in the Discovery toolbar.
   - Select **File** > **Options** in the Discovery menu bar. The system displays the Discovery Options dialog box
2. Click the **IP Discovery** tab at the top of the Options dialog box. The system displays the **IP Discovery** page of the Options dialog box.

3. Configure the IP Discovery options.
4. Click **Apply**.

Related topics:

IP Discovery field descriptions on page 104

IP Discovery field descriptions

The following table provides a list of the fields in the IP Discovery page of the Discovery Options dialog box.

Name	Description
Default gateway	The IP address of the default gateway used for Discovery. By default, this is the Gateway IP Address for the Network Management station.
Maximum subnet size to ping	The mask applied to the subnet address to determine the number of IP addresses in the subnet. Possible values are: • **Disable Ping** (Ping is not used to discover devices.) • **255.255.255.252** (2 hosts) • **255.255.255.248** (6 hosts) • **255.255.255.240** (14 hosts) • **255.255.255.224** (30 hosts) • **255.255.255.192** (62 hosts) • **255.255.255.128** (126 hosts) • **255.255.255.0** (254 hosts) • **255.255.254.0** (510 hosts) • **255.255.252.0** (1022 hosts) • **255.255.248.0** (2046 hosts) • **255.255.240.0** (4094 hosts) • **255.255.224.0** (8190 hosts) • **255.255.192.0** (16382 hosts) • **255.255.128.0** (32766 hosts) • **255.255.0.0** (65534 hosts) **Note:** The larger the maximum number of IP addresses per subnet the longer it takes for Discovery to finish.

Configuring the Discovery naming method

To configure the method the Discovery uses for selecting names for the discovered nodes:

1. Do one of the following:
   - Click  in the Discovery toolbar.
   - Select **File** > **Options** in the Discovery menu bar. The system displays the Discovery Options dialog box.
2. Click the **Names Discovery** tab at the top of the Discovery Options dialog box. The system displays the **Names Discovery** page of the Options dialog box.
3. Configure the Names Discovery options.
4. Click **Apply** to configure the Names Discovery options.

Related topics:

Names Discovery field descriptions on page 105

Names Discovery field descriptions

The following table provides a list of the fields in the Names Discovery page of the Discovery Options dialog box.

Name	Description
Update names for existing entries	This determines whether Discovery updates the names for nodes already listed in the Network Map. Possible states are: • Update - Discovery updates the names of all discovered nodes. User defined names are replaced by the best name discovered. • Don’t Update - The names of existing entries in the Network Map are not replaced.
Select best name sequence	This determines the order Discovery uses to define names for discovered nodes. Discovery can use the following sources to determine the name of a node: • IP - The IP address of the node. • SNMP system name - The value assigned to the device’s sysName MIB. • Name Service - The name assigned to the node via a Name Service application.

Name	Description
	Possible orders are: • **IP** - Discovery uses the IP address of the node as its name. • **SNMP sysName** > **IP** - If there is an SNMP system name, Discovery uses it as the node's name. Otherwise, Discovery uses the node's IP address. • **Name Service** > **SNMP sysName** > **IP** - If there is a Name Service defined name, Discovery uses it as the node's name. If there is no Name Service defined name, but there is an SNMP system name, Discovery uses it as the node's name. Otherwise, Discovery uses the node's IP address. • **SNMP sysName** > **Name Service** > **IP** - If there is an SNMP system name, Discovery uses it as the node's name. If there is no SNMP system name, but there is a Name Service defined name, Discovery uses it as the node's name. Otherwise, Discovery uses the node's IP address.

Selecting device types to discover

To configure the types of devices Discovery can find:

1. Do one of the following:
   - Click  in the Discovery toolbar.
   - Select **File** > **Options** in the Discovery menu bar. The system displays the Discovery Options dialog box.
2. Click the **Discovered Types** tab at the top of the Discovery Options dialog box.
3. Select the family of devices you want to discover. The available options are:
   - Communication Manager
   - Media Gateways and Switches
   - IP Office
   - Phone
   - Partner Devices
   - Others
4. Do one of the following:
   a. To add device types to the **Discovered Types** list:
      i. Select a device type from the **Undiscovered Types** list.

ii. Click . to move the device type to the **Discovered Types** list.

b. To remove device types from the **Discovered Types** list:

i. Select a device type from the **Discovered Types** list.

ii. Click to remove the device type from the **Discovered Types** list.

5. Click **OK** to configure the Discovered Types options.

Scheduling network discovery

The Discovery Scheduler can be used to set the Network Discovery to run at regular intervals and from specific start to end dates.

To schedule the network discovery:

1. Select **Actions** > **Schedule Network Discovery** in the Discovery menu bar. The system displays the Discovery Scheduler dialog box.
2. Configure the Discovery Scheduler options.
3. Click **Apply** to configure the Discovery Scheduler parameters.

Note:
Certain operations of theNetwork Management Console are disabled at different stages while the Network Discovery is running.

Related topics:

Discovery Scheduler field descriptions on page 107

Discovery Scheduler field descriptions

The following table provides a list of the fields in the Discovery Scheduler dialog box.

Name	Description
Enable Scheduler	When selected, the Discovery Scheduler is enabled.

Name	Description
Recurrence Pattern	The frequency to run Network Discovery. Possible values are: • **Hour** — Select the hourly interval between each discovery. • **Daily** — Select the daily interval between each discovery. • **Weekly** — Select the weekly interval between each discovery. • **Monthly** — Select the monthly interval between each discovery.
Start time	Select the time to start the scheduled discovery.
Range of recurrence	Select the start date and end parameter for the schedule. Possible end values are: • **No end date** • **End afteroccurrences** *x* — Enter the number of times after which the **Discovery Scheduler** does not run the Network Discovery. • **End by**- Enter the date after which the **Discovery Scheduler** does not run the Network Discovery.

Discovery of subnets and nodes

The Discovery function can be used to discover all the subnets and nodes in your network, or search for nodes on specific subnets.

For information on configuring the Discovery options, refer to Setting Discovery options on page 103.

Problems during the Discovery are reported in the Discovery log. For more information, refer to Using the Discovery log on page 113.

Related topics:

Discovering all subnets and nodes on page 108
Discovering nodes on specific subnets on page 109
Manually adding subnets on page 110
Modifying subnets on page 111
Subnet parameters on page 111
Deleting Subnets on page 112

Discovering all subnets and nodes

To discover all subnets and nodes:

1. Select **Actions** > **Start Network Discovery** or select **Edit** > **Delete All** in the Discovery menu bar to start the Discover process.
2. Click **OK** in the confirmation dialog box to delete all subnets in the Subnets table.
3. Click  in the Discovery toolbar.
   The progress of the discovery process is shown in the status bar of the user interface.
4. To stop the Discovery, click **Stop**.
5. Click **Yes** on the confirmation dialog box.
   The Discovery finishes adding the current node to the table and stops. When the Discovery finishes, the Subnets table contains a list of the subnets discovered in your network.
6. To save changes you make in the Discovery Subnets table, click  or select **File** > **Save changes**.

Discovering nodes on specific subnets

To discover nodes on a specific subnet:

1. Select the **Discover** check box for each subnet upon which you want to discover nodes or in the Subnets table, select the subnets upon which you want to discover nodes.
2. To select more than one subnet:
   a. Press **Shift** and select the last subnet in a contiguous selection.
   b. Press `Ctrl` and select additional subnets for a non-contiguous selection.
3. Click  in the Discovery toolbar or select **Edit** > **Select**
   The **Discover** check box for each selected subnet is selected.
   If the subnet you want to discover does not appear in the Subnets Table, add it manually. For more information on adding Subnets to the Subnets Table, refer to Manually adding subnets on page 110.
4. To deselect subnets upon which the Discovery can search for nodes, dlear the **Discover** check box for each subnet upon which you do not want to discover nodes or, iIn the Subnets Table, select the subnets upon which you do not want to discover nodes.

5. To deselect more than one subnet:
   a. Press **Shift** and select the last subnet in a contiguous selection.
   b. Press `Ctrl` and select additional subnets for a non-contiguous selection.
6. Click  in the Discovery toolbar or select **Edit** > **Unselect**.
   The **Discover** check box for each unselected subnet is cleared.
7. To start Discovery on the subnets whose **Discover** check box is selected, click  in the Discovery toolbar or select **Actions** > **Start Network Discovery** in the Discovery menu bar.
   The Discovery process begins searching for nodes on the subnets whose **Discover** check box is selected. The progress of the Discovery process is shown in the Status Bar of the user interface.
8. To stop the Discovery, click **Stop**.
9. Click **Yes** on the confirmation dialog box.
10. Click **Yes**. Discovery finishes adding the current node to the table and stops.
    The Discovery searches for nodes in the selected subnet. When the Discovery finishes, it updates the Subnets Table with the information discovered.
11. To save changes you make in the Discovery Subnets Table, click  or select **File** > **Save changes**.

Manually adding subnets

To manually add a subnet to the Subnets table:

1. Do one of the following:
   a. Click  in the Discovery toolbar.
   b. Select **Edit** > **Add** in the Discovery menu bar. The system displays the Add New Subnet dialog box.
2. Enter the subnet parameters in the dialog box. For information on the fields in the Add New Subnet dialog box, refer to Subnet parameters on page 111.
3. Click **Apply**. The subnet is added to the current Network map.
4. To save changes you make in the Discovery Subnets table, do one of the following:
   - Click  .

- Select **File** > **Save changes**.

Modifying subnets

To modify a subnet in the current Network Map:

1. Select a subnet in the Subnets Table.
2. Do one of the following:
   a. Click  in the Discovery toolbar.
   b. Double-click the selected subnet.
   c. Select **Edit** > **Modify** in the Discovery menu bar. The system displays the Modify Subnet dialog box.
3. Modify the parameters in the dialog box.
   For information on the fields in the Modify Subnet dialog box, refer to Subnet parameters on page 111.
4. Click **Apply** to modify the subnet in the current Network View.
5. To save changes you make in the Discovery Subnets Table, do one of the following:
   - Click  .
   - Select **File** > **Save changes**.

Subnet parameters

The following table provides a list of the parameters in the **Add New Subnet** and **Modify Subnet** dialog boxes.

Name	Description
Subnet IP	IP address of the subnet.

Name	Description
Subnet Mask/ Router	Determines whether a subnet mask or a specific router is used for the subnet. • **Subnet Mask** — A subnet mask is used for the subnet. You must enter a valid subnet mask in the **IP Subnet Mask** field. • **Router** — The subnet's router is used for the subnet. You must enter the router's IP address in the **Router** field. **Note:** Make sure that the **Actions** > **Dicovery Interfaces** check box is selected in case of a router-based discovery.
Subnet Mask	The IP of the subnet mask.
Router	The IP address of the subnet's router.
Discover	If selected, Discovery can search for nodes on the subnet.

Deleting Subnets

To delete a subnet:

1. Select a subnet in the Subnets table. To select multiple subnets, press `Ctrl` while selecting additional subnets.
2. Click  in the Discovery toolbar or select **Edit** > **Delete** in the Discovery menu bar.
3. Click **Yes** on the confirmation dialog box to delete the selected subnets from the Subnets table.

Discovering interfaces

To discover interfaces:

Select **Actions** > **Discover Interfaces** in the **Discover** menu bar.
When you select this option, you can query all SNMP-enabled devices for their IP interfaces and display them in the device list of Network Management Console. Also, the IP information of the directly connected subnets is automatically added to the

subnet list of the discovery window. However the system does not try to discover them by default.

If you do not select this option, you can discover only the primary management interface (PMI) of the supported device.

Using the Discovery log

The progress of the Discovery process is reported in the Discovery log. If the Discovery log contains entries, an “L” appears in the status bar of the Discovery window. Error entries are bolded in the Discovery log.

To view the Discovery log, do one of the following:

- Click  in the Discovery toolbar.
- Select **View** > **Discovery Log** in the Discovery menu bar. The system displays the Discovery log under the Subnets table.

Related topics:

Configuring router access parameters on page 113
Saving the Discovery log on page 114
Deleting log entries on page 115
Clearing the Discovery log on page 115

Configuring router access parameters

You can configure the SNMP parameters for a router that Discovery could not access. This enables the Discovery to search the router’s subnets for nodes.

To change the router access configuration and retry discovering nodes on the subnet:

1. Click the router's access error message in the Discovery log. The system displays the Router Access Configuration dialog box.
2. Change some of the router access configuration parameters.
3. Click **OK**. The router access configuration is changed, and Discovery tries to find nodes on the subnet. The dialog box contains the router access error message and the current router access configuration parameters.

Related topics:

Router Access Configuration field descriptions on page 114

Router Access Configuration field descriptions

The following table provides a list of the fields in the Router Access Configuration dialog box.

Name	Description
SNMP	The SNMP protocol. Possible SNMP protocols are: • SNMPv1 • SNMPv3
Read community	The read community of the router. Only applicable for SNMP protocol V1.
Write community	The write community of the router. Only applicable for SNMP protocol V1.
User	A user name as defined in the Secure Access Administration application. Only applicable for SNMP protocol V3.
Retries	The number of times Discovery pings the router with no response before giving up.
Timeout (milliseconds)	The amount of time (in milliseconds) Discovery pings the router with no response before timing out.

Saving the Discovery log

To save the Discovery log to a file:

1. Click  next to the Discovery log. The system displays the Save As dialog box.
2. Enter a filename, and browse to the directory in which to save the file.
3. Click **Save**.

Deleting log entries

To delete a log entry:

1. Select an entry. To select multiple entry, press `Ctrl` while selecting additional entries.
2. Click  next to the Discovery Log to delete the selected entries from the Discovery Log.

Clearing the Discovery log

To clear all entries from the Discovery Log:

1. Click  next to the Discovery Log.
2. Confirm your selection to clear the Discovery Log.

Chapter 12: Introduction to the Event Manager

Event Manager overview

Device agents send SNMP traps to theAvaya Network Management Server. These are received by the Event Manager. The Event Manager can be viewed using the Avaya Network Management Console. The Event log browser window of the Event Manager provides a list of traps in a table. Each row contains information about a single trap.

Note:

To receive device traps in Event Manager, include theAvaya Network Management Server on the list of each device's trap managers. For information on configuring the Avaya Network Management Server as a trap manager, refer to the device's User Guide or on-line help.

In addition, the Event Manager can notify multiple management hosts of network events. It can also open a pop-up message, play a sound file, or send an e-mail to notify managers of important network events. In addition, you can configure a network event to trigger a predefined script. The Event Configuration window of the Event Manager provides a method for defining actions and assigning actions to specific traps.

Viewing the Event Manager

To view the Event Manager, do one of the following:

- Click  .
- Select **Actions** > **Event Manager**. The system displays the Event Manager showing the Event Log browser.

Event Manager window

The Event Manager consists of the Event log browser window, Event Configuration window, and Action List window

Use the tabs at the top of the Event Manager to switch between the Event log browser and Event Configuration windows. The Action List window can only be viewed from the Event Configuration window.

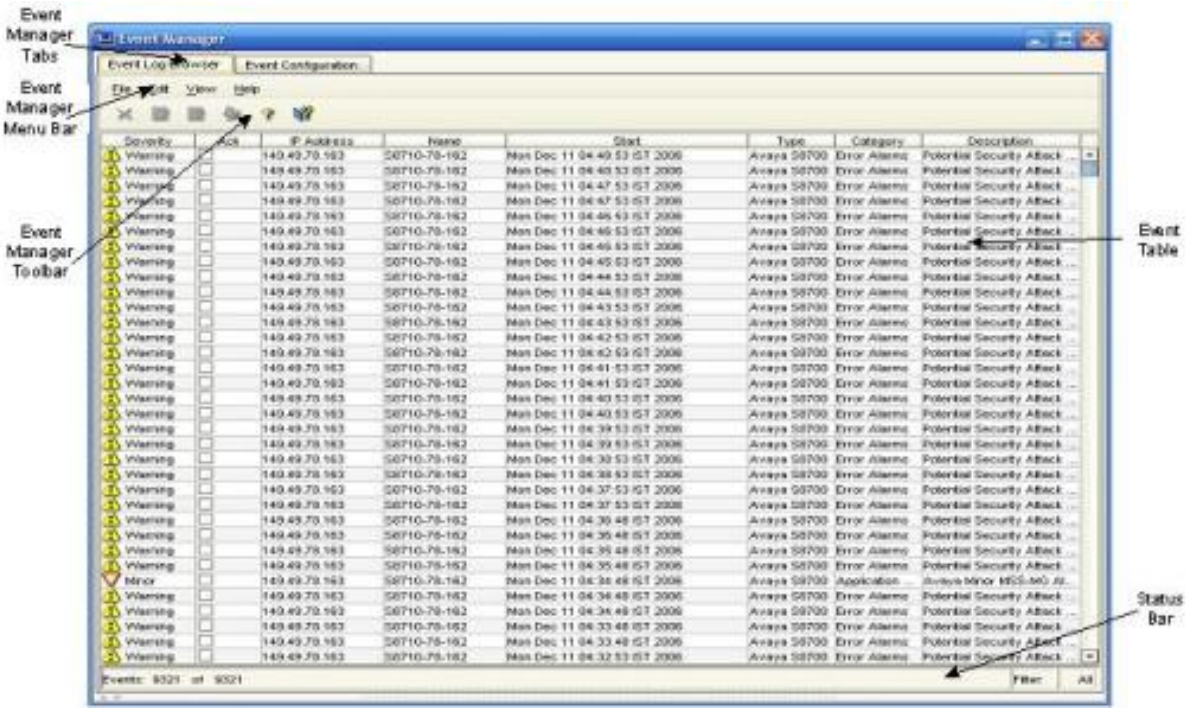
Related topics:

Event log browser window on page 118
Event Configuration window on page 121
Action List window on page 125

Event log browser window

The Event log browser window consists of the following elements:

- Event Manager Tabs — Tabs for switching between the Event log browser and the Event Configuration window.
- Menu bar — Menus for accessing Event log browser functions. For more information on Event Log Browser menus, refer to Appendix A: Network Management Menus.
- Event Log browser toolbar on page 119 - Toolbar buttons for accessing the Event log browser functions.
- Trap table on page 120- An area where a table of traps in the log opens.
- Event Log Browser Status Line on page 121 - Displays information about the number of traps in the Event log browser.



Related topics:

[Event Log browser toolbar](#) on page 119
[Trap table](#) on page 120
[Event Log Browser Status Line](#) on page 121

Event Log browser toolbar

The table below describes the buttons on the Event Log Browser Toolbar and gives the equivalent menu options.

Button	Description	Menu Item
	Deletes the selected traps.	**Edit** > **Delete**
	Marks the selected traps as acknowledged.	**Edit** > **Acknowledge**
	Marks the selected traps as unacknowledged.	**Edit** > **UnAcknowledge**
	Highlights the selected trap in the tree in the Event Configuration window.	**Edit** > **Modify Event**
	Filters the information in the trap log by the criteria you select.	

Button	Description	Menu Item
	Opens the context-sensitive help.	**Help** > **Help On**

When you place the cursor on a toolbar button for one second, a label appears with the name of the button.

Trap table

By default, the Trap Table lists the traps sent to the Network Management Server in the order in which they were sent. However, you can sort the Trap Table by any of its fields. To sort the Trap Table by one of its fields, click the field's column header. To reverse the sort order, click the column header again.

You can configure the information in the Trap table using the **Assign Action Form** area in the Event Configuration window, refer to Assign Action form area on page 123.

Note:

The Trap Table can hold up to 10,000 traps.

The following table provides a list of the fields in the Trap Table and an explanation of each field.

Name	Description
Severity	An icon representing the severity of the trap: • - Info • - Warning • - Minor • - Major • - Critical
Ack (Acknowledged)	This column shows a checkmark if a trap has been acknowledged.
IP Address	The IP address of the sender of the trap.
Name	The best name of the sender of the trap.
Start	The time the trap was sent.
Type	The type of device from which the trap was sent.
Category	The category of the event.
Description	A description of the trap. The information displayed in this field is configured in the Assign Action Form Area of the Event Configuration User Interface. For more information, refer to Assign Action form area on page 123.

To locate the device from which an event was sent, double-click the event in the Trap table and the device is highlighted in the SNMP Console tree.

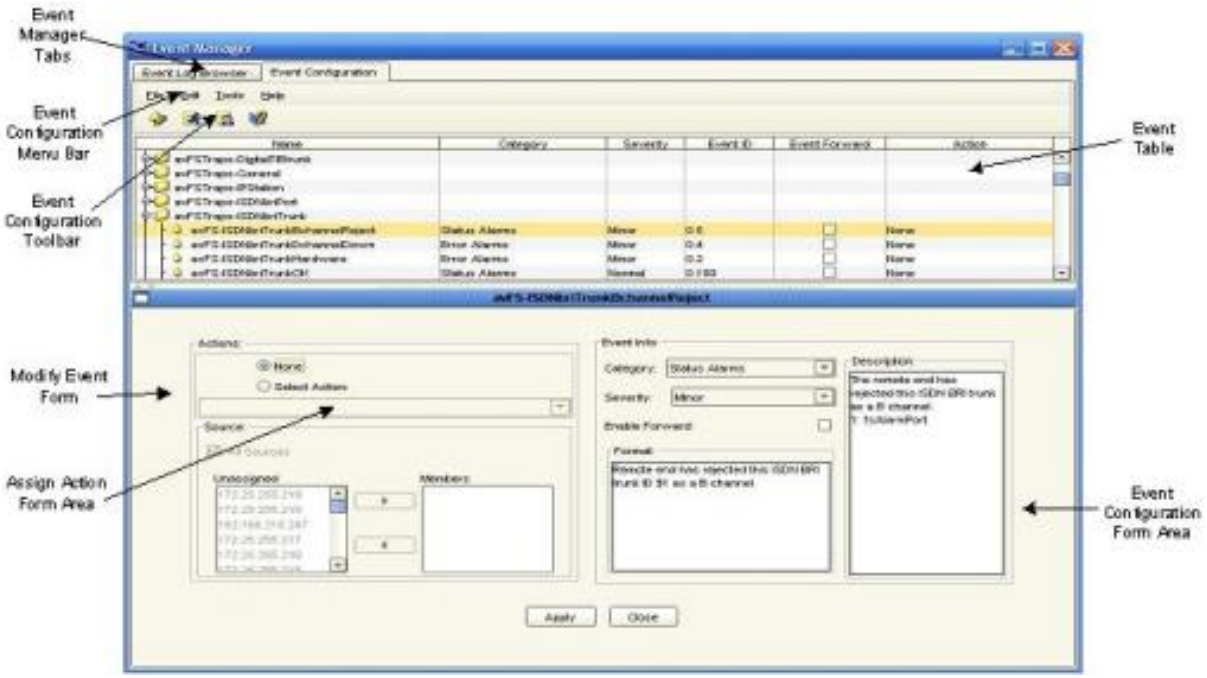
Event Log Browser Status Line

The Event log browser's status line displays the number of traps in the Event log browser. This number includes traps that are not currently displayed in the Trap table. In addition, the status line displays the current filtering options.

Event Configuration window

The Event Configuration window consists of the following elements:

- Event Manager Tabs — Tabs for switching between the Event log browser and the Event Configuration window.
- Menu bar — Menus for accessing the Event Configuration functions. For more information on the Event Configuration menus, refer to Appendix A: Network Management Menus.
- Event Configuration toolbar on page 122 - Toolbar buttons for accessing the Event Configuration functions.
- Event table on page 123 - A collapsible table providing a list of trappable network events and their configured responses.
- Assign Action form area on page 123 - An area that contains the following dialog boxes:
    a. Assign Action Form — used to assign actions to specific events.
    b. Event Configuration Form — used to configure the display of events in the Event log browser.



Related topics:

Event Configuration toolbar on page 122
Event table on page 123
Assign Action form area on page 123
Event Configuration form area on page 124

Event Configuration toolbar

The table below describes the buttons on the Event Configuration toolbar and gives the equivalent menu options.

Button	Description	Menu Item
	Opens the Modify Trap dialog box for the selected network event.	**Edit** > **Modify Event**
	Opens the Action List window.	**Tools** > **Action List**
	Opens the Event Forwarding dialog box.	**Tools** > **Event Forwarding**
	Opens the context-sensitive help.	**Help** > **Help On**

When you place the cursor on a toolbar button for one second, a label appears with the name of the button.

Event table

The Event table lists network events in a collapsible tree. Each event category can be expanded or collapsed by clicking the handle next to the category. The following table provides a list of the fields in the Event table and an explanation of each field.

Name	Description
Name	The name of the event or event category.
Category	The category of the event.
Severity	The severity of the network event: • Normal • Warning • Minor • Major • Critical
Event ID	A numeric identifier for the event.
Event Forward	The state of event forwarding for the trap. If the check box is selected, the event is configured for forwarding. If the check box is not selected, the event has not been configured to be forwarded. **Note:** If event forwarding is configured for all traps, the **Event Forward** check box is not relevant. All network events are forwarded.
Action	The defined action triggered by the event.

Note:
When running the Network Management from a remote station, the Event table is read-only.

Assign Action form area

The Assign Action Form area provides a dialog box for assigning pre-defined actions to specific events. The following table provides a list of the fields in the Assign Action Form and an explanation of each field.

Name	Description
Actions	The action assigned to the selected event. Possible actions are: • None - No action is assigned to the selected event. • Select Action - The action displayed in the drop-down list is assigned to the selected event.
Source	The IP addresses of the sources of the selected event. Only if the selected event's trap is sent from one of the IP addresses listed in the **Members** list does the configured action occur. If **All Sources** is checked, the configured action occurs regardless of the source from which the trap is sent.

Event Configuration form area

The Event Configuration area allows you to configure the information displayed in the Event log browser.

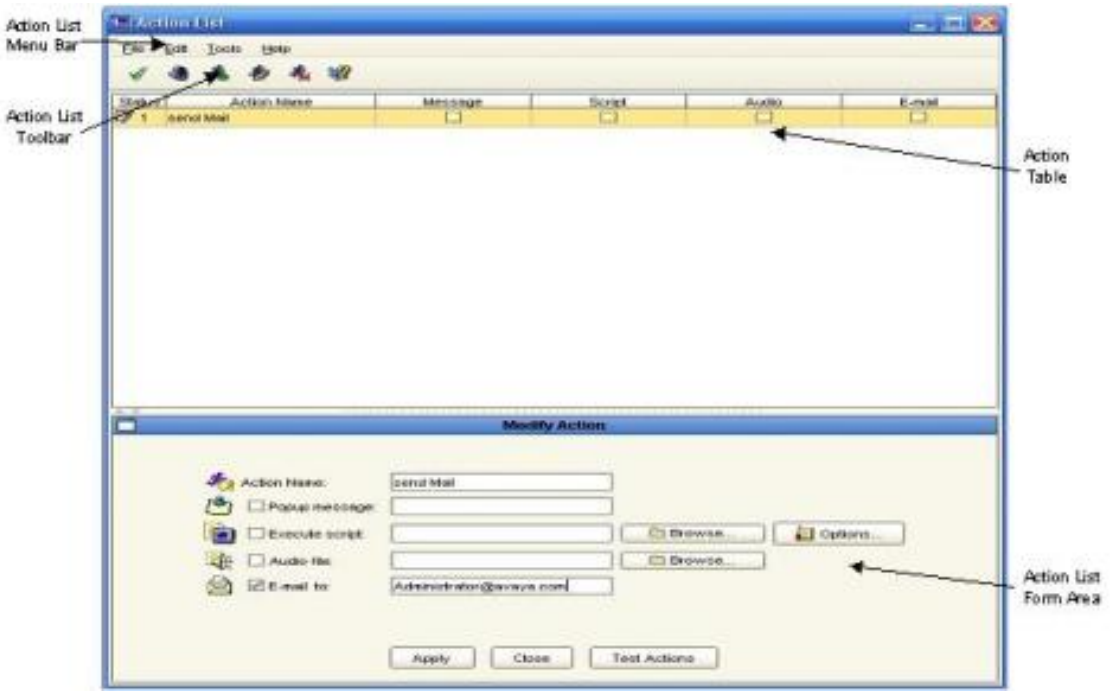
Name	Description
Category	The type of event: • Log Only • Ignore (default for generic SNMP traps) • Error Alarms • Threshold Alarms • Status Alarms • Configuration Alarms • Application Alert Alarms • Network Topology Alarms **Note:** Traps defined for Log Only and Ignore are not shown in the event browser.
Severity	The severity of the selected event: • Normal • Warning • Minor • Major • Critical
Enable Forward	If selected, the event is forwarded to selected stations. If cleared, the event is not forwarded, unless you forward all events.

Name	Description
Format	The format in which the event is displayed in the description field of the Event log browser. The following parameters are available for configuring the format: • **$e** — trap enterprise. • **$<number>** — retrieves the specified parameter from the trap. <number> denotes the order in which the parameter appears. (I.e., the first parameter is denoted by '1', the second parameter is denoted by '2', etc.) • **$A** — IP address of the agent who sent the trap. • **$#** — returns the number of parameters in the trap. • **$*** — enterprise:interface number. All arguments are separated by a colon. • **$E** — OID trap alias (i.e., the name of the group in which the trap is defined).
Description	A detailed description of the selected event. This information does not appear in the Event log browser.

Action List window

The Action List user interface consists of the following elements:

- Menu bar - Menus for accessing Action List functions. For more information on the Action List menus, refer to Appendix A: Network Management Menus.
- Action List toolbar on page 126 - Toolbar buttons for accessing the Action List functions.
- Action table on page 127 - A table providing a list of configured responses to the network events.
- Action Form Area on page 127 - An area where all dialog boxes open.



Related topics:

Action List toolbar on page 126
Action table on page 127
Action Form Area on page 127

Action List toolbar

The table below describes the buttons on the **Action List** toolbar and gives the equivalent menu options.

Button	Description	Menu Item
	Applies the changes to the Action List.	**Edit** > **Apply**
	Undoes all unapplied changes to the Action List.	**Edit** > **Revert**
	Adds a new action to the Action List.	**Edit** > **Add**
	Opens the Modify Action dialog box for the selected action.	**Edit** > **Modify**
	Deletes the selected action.	**Edit** > **Delete**
	Opens context-sensitive help.	**Help** > **Help on**

When you place the cursor on a toolbar button for one second, a label appears with the name of the button.

Action table

The Actiont table lists configured actions. Each row in the table represents an action that can be assigned to a trap. These actions are listed in the **Action Form Area** in the Event Configuration window. The following table provides a list of the fields in the Action table and an explanation of each field.

Name	Description
Status	The status of the row in the table. For more information, refer to Using the Avaya Network Management Console tables.
Action Name	The user defined name of the action.
Message	If selected, the action includes a pop-up message.
Script	If selected, the action includes running a script.
Audio	If selected, the action includes an audible message.
E-mail	If selected, the action includes sending an e-mail.

Note:
When running the Network Management from a remote station, the Action table is read-only.

Action Form Area

The Action Form area is where the Add Action and Modify Action dialog boxes open. For information on the fields in the Add Action and Modify Action dialog boxes, refer to Action fields on page 137.

Closing the Event Manager

To close the Event Manager:

1. Select **File** > **Exit**. The Event Manager closes.

Chapter 13: Managing events

Configuring the Event Log to discard or archive old events

The Event Log can hold up to 10,000 events. When this limit is reached, events must be removed from the Event Log to provide room for new events. You can configure the Network Management to either discard old events or archive them.

Note:
By default, when the Event Log holds 10,000 events, the oldest 1,000 events are discarded.

Note:
Archived events are appended to the event archive.

To configure the method Network Management uses to clean up the Event Log:

1. Select **File** > **Option**. The system displays the Event Log Options dialog box.
2. Enter a number between 1 and 9999 in the **Events to remove from the event Log:** field. This is the number of events to be deleted when there are 10,000 events in the Event Log.
3. If you want the deleted events saved to an archive, select the **Archive events** check box and then do one of the following:

   Enter a path and file name for the event archive in the **Archive File name** field. Ensure that the file extension is either `csv` for a Comma Separated Value file or `xml` for an XML file.

   Perform the following tasks:

   i. Click **Browse**. The system displays a file browser dialog box.
   ii. Browse to the directory in which you want to save the archive.
   iii. Enter a file name in the **File name** field.

iv. Select a file type from the **Files of type** drop-down list. Available file types are CSV (comma separated value) and XML.

4. Click **Apply** to configure the clean up method for the Event Log. Whenever the Event Log contains 10,000 events, this method is used to remove the specified number of events from the Event Log.

Note:

If you specify a CSV file for the event archive and the file is open when events need to be archived, a new file is created containing all of the events in the old archive. Archiving continues using the new file.

About filtering events

By default, all events in the Event Log browser are displayed in the Event table. However, you can filter events by severity level, category, source, device type, or acknowledgment status. When you filter the Event table, events that do not meet the filtering criteria are hidden. However, they are not deleted from the Event Log.

Note:

You can only filter by one criterion at a time.

Related topics:

Filtering events by security level on page 130
Filtering by category on page 131
Filtering by IP address on page 131
Filtering by device type on page 132
Filtering by acknowledged on page 132
Viewing all events on page 133

Filtering events by security level

To filter events by security level, do one of the following:

1. Perform the following steps:
   a. Select **View** > **Filter** > **Severity Filter** to display the Severity Filter dialog box.
   b. Select the check box next to the severity levels of the events you want displayed in the Event table.

c. Click **Apply** to display the events of the selected severity levels in the Event table.

2. click  and then click the **Severity** column of an event with the desired severity to display only events with the selected severity in the Event table.

Filtering by category

To filter by category, do one of the following:

1. Perform the following steps:
   a. Select **View** > **Filter** > **Category Filter**. The system displays the Category Filter dialog box.
   b. Select the category of the devices from which you want to view events from the listbox.
   c. Click **Apply** to display events from the selected category in the Event table.
2. Click  and click the **Category** column of an event from the desired device to display events from the selected category in the Event table.

Filtering by IP address

To filter by IP address, do one of the following:

1. Perform the following steps:
   a. Select **View** > **Filter** > **IP Address Filter**. The system displays the IP Address Filter dialog box.
   b. Select the IP addresses of the devices from which you want to view events from the listbox.

c. Click **Apply** to display events from the selected IP addresses in the Event table.

2. Click  and then click the **From** column of an event from the desired device to display events from the selected IP address in the Event table.

Filtering by device type

To filter by device type, do one of the following:

1. Perform the following steps:
   a. Select **View** > **Filter** > **Device Type Filter**. The system displays the Device Type Filter dialog box.
   b. Select device types from the listbox.
   c. Click **Apply** to display events from devices of the selected types in the Event table.
2. Click  and click the **Device Type** column of an event from the desired device type to display events from devices of the selected device type in the Event table.

Filtering by acknowledged

To filter acknowledged events, do one of the following:

1. Perform the following steps:
   a. Select **View** > **Filter** > **Acknowledge Filter**. The system displays the Acknowledged Filter dialog box.
   b. Select the check box next to the Acknowledgement statuses of the events you want displayed in the Event table.

c. Click **Apply** to display events with the selected Acknowledgement statuses in the Event table.

2. Click  and then click the **Ack** column of an event with the desired Acknowledgement to display events with the same value in the **Acknowledged** field in the Events table.

Viewing all events

To cancel the current filtering options and view all events in the Event table:

Select **View** > **Filter** > **No Filter**.

Acknowledging events

It is useful to acknowledge events of which you are aware, even if you do not want to delete them. This can help focus your interest on events that you have not yet seen.

To acknowledge an event:

1. Select an event.
   - To select multiple events, press `Ctrl` while selecting additional events.
   - To select all events, select **Edit** > **Select All**.
2. Do one of the following:
   - Click  .
   - Select **Edit** > **Acknowledge**.
   - Click the **Acknowledge Icon** field in a event that was not yet acknowledged. The event is marked with a checkmark.

Related topics:

Removing the acknowledge mark from a event on page 134

Removing the acknowledge mark from a event

To remove the acknowledge mark from a event:

1. Select an event.
   - To select multiple events, press `Ctrl` while selecting additional events.
   - To select all events, select **EditSelect All**.
2. Do one of the following:
   - Click  .
   - Select **Edit** > **UnAcknowledge**.
   - Click the **Acknowledge Icon** field in an acknowledged event. The event is unmarked.

Deleting events

It is important to delete old events from the Event Table. This prevents the Event Manager from becoming unwieldy and allows you to focus on current network events.

To delete an event:

1. Select an event.
   - To select multiple events, press `Ctrl` while selecting additional events.
   - To select all events, select **Edit** > **Select All**.
2. Click  or select **Edit** > **Delete**.
3. Click **Yes** on the confirmation dialog box to delete the event.

Editing severity levels

You can change the severity level of selected events. This is useful when a event is more (or less) important than it would be normally. The change in importance may be the result of an

extraordinary load on the network, the event's source being a monitored port, or any other cause.

To edit the severity level:

1. Select an event.
2. Select **Edit** > **Change Severity** > **Change severity to *Severity level*** , where *Severity level* is the severity level for the event. Or select a severity level from the event's **Severity** column. The event's severity level is changed.

Saving the Event table

The Event table can be saved to a file. The file can be in one of the following formats:

- Comma Separated Values (CSV) — As a text file with the columns in each row separated by commas.
- XML — As an XML file.

To save the Event table to a file:

1. Click **File** > **Export**. The system displays the Export dialog box.
2. Browse to the directory in which to save the file.
3. Enter a name for the file in the **File Name** field.
4. Select the file format from the **Files of Type** drop-down list.
5. Click **Save**.

Actions overview

Actions are methods of notifying managers of important network events. Notification methods include the appearance of a pop-up window, the running of a script, the playing of a sound file, and the sending of an e-mail.

A defined action can include any combination of these notification methods. Once an action is defined, it can be assigned to selected events. For more information on assigning actions to events, refer to Configuring Events on page 140.

The Action table includes a list of all configured actions.

Adding Actions

To add an action to the Action List:

1. Do one of the following: .
   a. Click 
   b. Select **Edit** > **Add**.

   The system displays the **Add Action** dialog box.
2. Define the action using the **Add Action** dialog box fields. For information on the fields in the**Add Action** dialog box, refer to Action fields on page 137.
3. To test the new action, click **Test Actions**. The defined actions occur.
4. Click **Apply** to add the action to the Action List.

Modifying Actions

To modify an action in the Action List:

1. Select an action in the Action List.
2. Do one of the following:
   a. Click  .
   b. Select **Edit** > **Modify**. The system displays the Modify Action dialog box.
3. Edit the action using the Modify Action dialog box. For information on the fields in the Modify Action dialog box, refer to Action fields on page 137.
4. To test the modified action, click **Test Actions**. The defined actions occur.
5. Click **Apply** to modify the action in the Action List.

Action fields

The following table provides a list of the fields in the Add Action and Modify Action dialog boxes and an explanation of each field.

Name	Description
Action Name	The name of the defined action.
Popup message	The state of the check box determines whether the action includes a pop-up message. The text box contains the text of the pop-up message.
Execute script	The state of the check box determines whether the action includes running a script. The text box contains the name of the script file. You can assign a script file by clicking **Browse** and using the standard file browser to find the script file. For more information on scripts, refer to Action scripts.
Audio file	The state of the check box determines whether the action includes playing an audio file. The text box contains the name of the audio file. You can assign an audio file by clicking **Browse** and using the standard file browser to find the audio file. For more information on audio files, refer to Action audio files on page 139.
E-mail to	The state of the check box determines whether the action includes sending an e-mail. The text box contains the address to which the e-mail is sent. You can include more than one email address, each separated by a semicolon.

Related topics:

Actions scripts on page 137
Action audio files on page 139

Actions scripts

You can include any executable file in an action. Valid executable files are operating system dependant. For example, on a computer running Windows, BAT, COM, and EXE files are executables.

In addition, up to four variable command line parameters can be included in the command.

Related topics:

Adding command line parameters to the script on page 138

Adding command line parameters to the script

To add command line parameters to the script:

1. Do one of the following:
   - Enter the parameters manually in the **Execute Script** field.
   - Click **Options**. The system displays the Script Parameters dialog box.
2. Select the check box next to the parameters you want to add to the command.
3. Click **Apply**. The Script Parameters dialog box closes, and the selected parameters are inserted in the **Execute Script** field.

   In addition, you can add command line parameters, specific to your system.

   For example, the command **`print_report printer:BOSTON $A $e $f`**, may send the command `print_report printer:BOSTON 213.21.70.142 Major "Bus 10 internal clock fault"` to your computer.

Note:
The Network Management is not responsible for validating any assigned scripts or ensuring that they can receive command line parameters.

Related topics:

Command line variables on page 138

Command line variables

Parameter	Variable	Description
IP Address	*$A*	The IP address of the device from which the event was sent.
SysOId + n	*$e*	The SysOId of the device followed by `.n` for predefined events, or **0**.n for vendor specific events, where `n` is the event code.
Severity	*$s*	The severity of the event.
Event Message	*$f*	A formatted message describing the event.

Action audio files

You can select any audio file recognized by your computer for inclusion in an action. The file is played by its associated application. If the file format is unrecognized by your operating system, an error occurs.

Note:
The Network Management is not responsible for validating an audio file or format.

Deleting Actions

To delete an Action:

1. Select an action in the Action list.
2. Do one of the following:
   - Click  .
   - Select **Edit** > **Delete** to mark the selected action for deletion in the Action list.

Applying changes to the Action list

To apply the changes to the network:

Do one of the following:

- Click  .
- Select **Edit** > **Apply** to apply the changes to the network.

Defining email settings for Actions that include email

If you define actions that include e-mails, you must configure the Avaya Network Management Console to use an appropriate SMTP server. In addition, you should specify an e-mail address as the sender of the e-mail.

To define email settings:

1. Select **Tools** > **Options**. The system displays the **Action List Options** dialog box.
2. Enter your SMTP server in the **SMTP Server** field.
3. Enter the e-mail address you want to appear as the sender of e-mails in the **Sender Address** field.
4. Click **Apply** to configure the Avaya Network Management Console to use the specified SMTP server.

Configuring Events

Some network events are so important, that the reporting of the event in the Event Log Browser is not sufficient. The Event Configuration window allows you to configure additional notification methods for important events. In addition, you can configure event forwarding from the Event Configuration window.

To configure events and event forwarding, click the **Event Configuration** tab. The system displays the Event Configuration window. For information on the Event Configuration user interface, refer to Event Configuration window on page 121.

Related topics:

Assigning actions to events on page 140
Configuring Event Forwarding on page 142

Assigning actions to events

To assign an action to an event:

1. Click the handle next to the category of the event for which you want to define an action.
2. Select the event for which you want to define an action.
3. Do one of the following: .
   a. Click 
   b. Select **Edit** > **Modify Event**. The system displays the Action Definition dialog box under the Event Configuration window.
4. Click **Select Action**. To unassign an action, click **None**, and continue with Step 7 on page 0 .
5. Select a defined action from the drop-down list.
6. Select source devices for the action. The Event Action is defined for only the devices in the **Members** drop-down list for all devices.

   To define the action for all network devices, select the **Add All Sources** check box.

   - To add individual devices to the **Members** list, select a device in the **Unassigned** list and click  . The selected devices are moved to the **Members** list.
   - To remove individual devices from the **Members** list, select a device in the **Members** list and click  . The selected devices are moved to the **Unassigned** list.

   Note:

   To select a contiguous group of devices, press the `Shift` key and select the last device in the group.

   To select a non-contiguous group of devices, press the `Ctrl` key while selecting additional devices.
7. Select a category from the **Category** drop-down list.
8. Select a severity from the **Severity** drop-down list.
9. If you want to enable event forwarding for the event, select the **Enable Event Forward** check box.

   The event is forwarded to the IP addresses listed in the **Event Forwarding Options** dialog box. To prevent the event from being forwarded, clear the **Enable Event Forward** check box. The event is not forwarded unless the **All** button is selected in the Event Forwarding Options dialog box.
10. Define the format in which to display the event in the Format area.

11. Enter a description of the event in the Description area.
12. Click **Apply** to assign the selected action to the selected event from the selected source.

Note:
Only one action can be assigned to a particular event.

Configuring Event Forwarding

Event forwarding enables events to be posted to devices further up the network hierarchy. This is useful, because it minimizes the need to configure multiple event recipients on the device level. Instead, events from multiple devices can be forwarded to a single network device from which the events can be sent to multiple recipients. In addition, you can forward all events or only specific events.

Related topics:
Opening the Event Forwarding Options dialog box on page 142

Opening the Event Forwarding Options dialog box

To open the **Event Forwarding Options** dialog box, do one of the following:

- Click  .
- Select **Tools** > **Event Forwarding**. The system displays the Event Forwarding Options dialog box.

Related topics:
Configuring event forwarding sources on page 142
Configuring forwarding recipients on page 143

Configuring event forwarding sources

To configure the event forwarding sources:

1. Do one of the following:
   - To forward all events, select the **Forwarding All Events** check box.

- To forward only specific events, clear the **Forwarding All Events** check box. Only events configured with the **Enable Event Forward** check box in the **Action Definition** dialog box are forwarded. For more information, refer to Defining email settings for Actions that include email on page 140.

2. Select the severity level of the alarm: Critical, Major, Minor, Warning, Info. You can select any number of levels.
3. Select the event Format: **SNMPv1 event, Syslog**.
4. Click **Apply** to configure the Event forwarding sources.

Configuring forwarding recipients

You can configure up to ten devices to receive forwarded network events. You can perform following tasks:

---

1. To add devices to the Recipients List:
   a. Click  . A row is added to **Customized Source** list.
   b. Enter the IP address and port, separated by a colon, of a device to which you want to forward network events. The default port for SNMPv1 is 162, and for Syslog is 514.
   c. Click **Apply**. The recipient is added to the **Customized Source** list.
2. To modify a device's information in the **Customized Source** list, change the recipient's IP address in the **Customized Source** list and click **Apply**. The device's information is modified.
3. To remove devices from the **Customized Source** list:
   a. Select the row with the device's IP address in the **Customized Source** list.
   b. Click  .
   c. Click **Apply** to remove the device from the **Customized Source** list.

Chapter 14: Introduction to the NM Log Viewer

NM Log Viewer overview

The NM Log Viewer is used to display log files generated by the Network Management applications in a user-friendly tabular format. The log file contains information about actions performed and events taking place in the Network Management Offer.

For example, while creating/deleting Network Maps, manually adding/deleting/modifying devices in the network or updating the Network Management Console view, the actions are logged to the log files. The details of the log can be viewed using the NM Log Viewer utility.

The NM Log Viewer allows you to sort the logs by columns (by clicking the table header). The NM Log Viewer supports filtering of the logs according to their severity. For example, if you want to view logs with only the ERROR level, then you can set the filter to show only the ERROR level logs.

You can export these logs to a .csv or .xml file. These logs can be useful for security audits and to diagnose problems.

Note:
This utility supports only log4j formatted logs.

Launching the NM Log Viewer

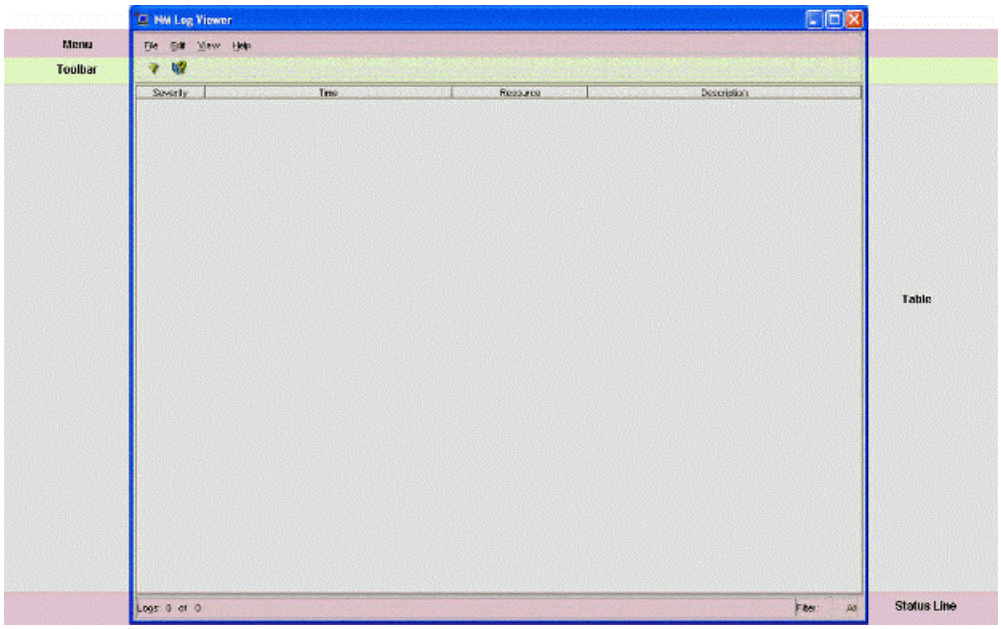
To launch the NM Log Viewer, do one of the following:

- Click  .
- From the Network Management Console window, select **Actions** > **NM Log Viewer** to launch the NM Log Viewer, displaying the NM Log Viewer table.

NM Log Viewer window

The NM Log Viewer user interface consists of the following elements:

- Menu Bar – Menus for accessing the NM Log Viewer functions. For more information on the NM Log Viewer menus, refer to Appendix A: Network Management Menus
- NM Log Viewer toolbar on page 146 — Toolbar buttons for accessing the NM Log Viewer functions.
- NM Log Viewer table on page 147 — Displays the logs in a tabular format in the order they were logged.
- NM Backup Utility Status Line on page 163 — Displays information about the number of logs in the NM Log Viewer.



Related topics:

NM Log Viewer toolbar on page 146
NM Log Viewer table on page 147
NM Log Viewer Status Line on page 148

NM Log Viewer toolbar

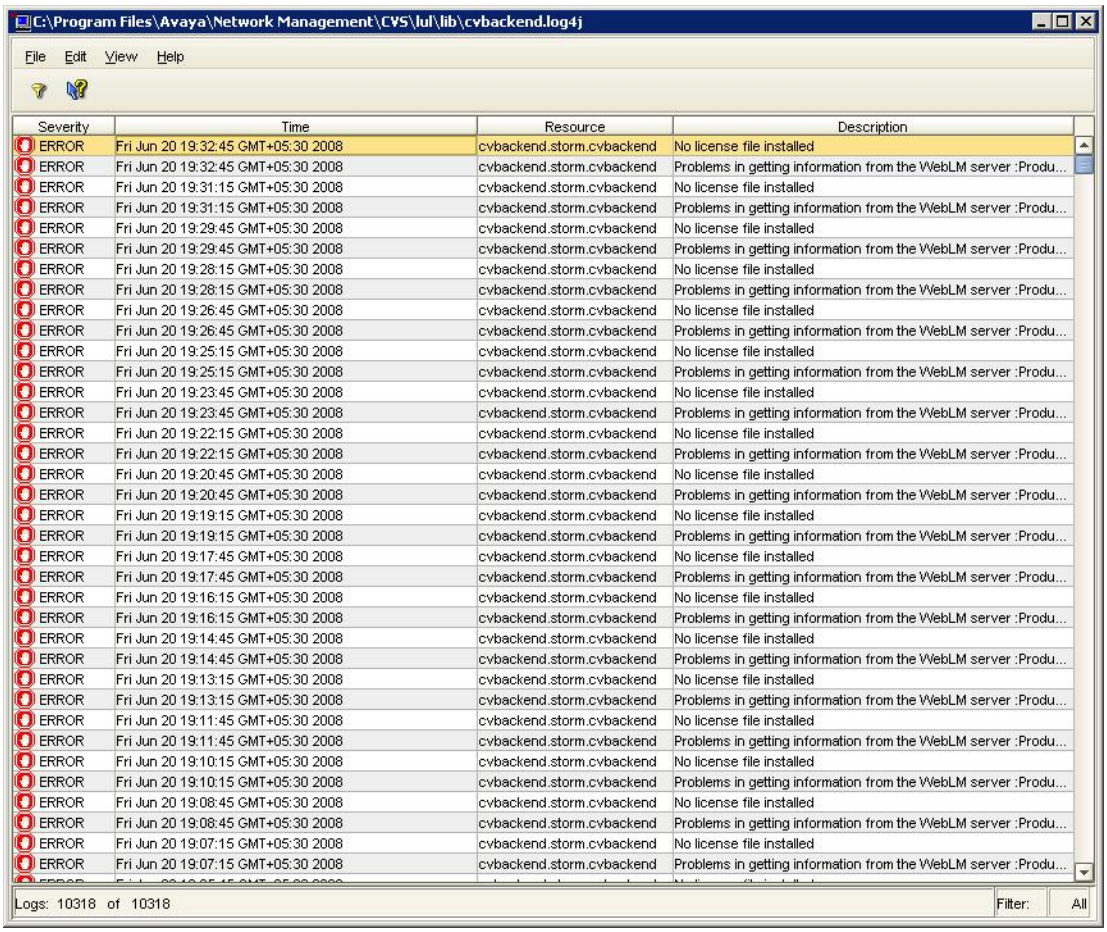
The table below describes the buttons on the NM Log Viewer toolbar and gives you their equivalent menu options.

Table 1: NM Log Viewer Toolbar

Button	Description	Menu Item
	Filters the information in the log by Severity.	**View** > **Filter** > **Severity Filter**
	Opens context-sensitive help.	**Help** > **Help On**

NM Log Viewer table

By default, the NM Log Viewer table lists the logs in the order in which they were logged. However, you can sort the NM Log Viewer table by any of its fields. To sort the NM Log Viewer table by one of its fields, click the field's column header. To reverse the sort order, click the column header again.



The following table provides a list of the fields in the NM Log Viewer table and an explanation of each field.

Name	Description
Severity	An icon representing the severity of the log: • - Info Severity • - Warn Severity • - Debug Severity • - Error Severity • - Fatal Severity
Time	The date and time of the log
Resource	The source of the log
Description	A description of the log

NM Log Viewer Status Line

The NM Log Viewer's Status Line displays the number of logs in the NM Log Viewer table. This number includes logs that are not currently displayed in the NM Log Viewer table. In addition, the Status Line displays current filtering options.

Chapter 15: Managing Logs in the NM Log Viewer

Filtering logs

By default, all logs in the NM Log Viewer are displayed in the NM Log Viewer table. However, you can filter logs by severity level. When you filter the Log table, logs that do not meet the filtering criteria are hidden. However, they are not deleted from the log.

Related topics:

Filtering logs by security level on page 149
Viewing all logs on page 150

Filtering logs by security level

To filter logs by security level:

1. Click or select **View** > **Filter** > **Severity Filter**. The system displays the Severity Filter dialog box.



2. Select the check box next to the severity levels of the logs you want displayed in the NM Log Viewer table.
3. Click **Apply** to display the logs of the selected severity levels in the NM Log Viewer table.

Viewing all logs

To cancel the current filtering options and view all logs in the NM Log Viewer table:

Select **View** > **Filter** > **No Filter**. All logs are displayed in the NM Log Viewer table.

Exporting logs

The logs displayed in the NM Log Viewer can be exported to a file. The file can be saved in one of the following formats:

- Comma Separated Values (CSV) — As a text file with the columns in each row separated by commas.
- XML — As an XML file.

To export logs:

1. Click **File** > **Export**. The system displays the Export dialog box.
2. Browse to the directory in which you want to save the file.
3. Enter a name for the file in the **File Name** field.
4. Select the file format from the **Files of Type** drop-down list.
5. Click **Save** to save the logs to the specified file.

Opening logs

You can open the log files generated by the Network Management Server using the NM Log Viewer.

To open logs:

1. In the NM Log Viewer window, select **File** > **Open**. The system displays the Open dialog box.
2. Browse to the directory where the logs are saved.
3. Select the log file you want to open.
4. Click **Open**.

Related topics:

Resolving the Out of Memory error on page 151

Resolving the Out of Memory error

Occasionally, while opening large Network Management application log files (around 10 MB size), you may encounter the OutOfMemory error. The NM Log Viewer window does not respond for a long time (over 20 seconds).

To fix this error:

1. Open the Java console. To open Java console, do one of the following:
   - Right-click the java icon on the system tray, and click **Open Control Panel**.

- Select **Start** > **Control Panel** > **Java**. The system displays the Java Control Panel dialog box.

2. Click the **Java** tab.
3. Click **View** under the **Java Applet Runtime Settings** area of the Java Control Panel dialog box. The system displays the Java Runtime Settings dialog box.
4. Double-click the **Java Runtime Parameters** text box in the table for version 1.6.0_16. Network Management 6.0 uses JRE version 1.6.0_16. The cursor is shown on the text box and you can now enter the runtime parameters.
5. The default maximum heap size for JRE 1.6.0_16 is 64MB. Increase the heap size to 128MB or higher, using the –Xmx128m option. The command line java parameter for setting the maximum heap size is as below:

   ```
   -Xmx<size> set maximum Java heap size
   ```

6. Click **OK**.

Note:

The NM Log Viewer cannot open log files on the server if it is launched from a client machine. The logs need to be available locally or on a shared network drive. The NM Log Viewer does not manipulate the content of the open log files.

Closing the NM Log Viewer

To close the NM Log Viewer:

Select **File** > **Exit**, or click the NM Log Viewer's application close button. The NM Log Viewer closes.

Chapter 16: Introduction to the Quick Log Viewer

Quick Log Viewer overview

The Network Management Console keeps a log of important events and activities performed within the network. The Quick Log Viewer allows you to quickly view the important events taking place in the system.

The logs are displayed in a tabular format. You can choose to sort, delete, clear and save the logs from the Quick Log Viewer table.

Launching the Quick Log Viewer

To launch the Quick Log Viewer :

Double-click thE **Quick Log Viewer** section of the Network Management Console status bar. The system displays the Quick Logs Viewer window.



Related topics:

Quick Log Viewer table on page 154
Quick Log Viewer toolbar on page 154

Quick Log Viewer table

The Quick Log Viewer table lists the logs in a tabular format. You can sort the table by any of its fields. To sort the table by one of its fields, click the field's column header. To reverse the sort order, click the column header again.

The following table provides a list of the fields in the Quick Log Viewer table and explanation of each field.

Name	Description
#	Serial number of the log in the table.
Severity	Severity level of the log. • WARN • ERROR • INFO • FATAL • DEBUG
Application	Name of the application
User	Name of the user
Event Type	The type of event occured
Message	Description of the log.
Date Time	Date and time of the log.

Quick Log Viewer toolbar

The table below describes the buttons on the Quick Log Viewer toolbar.

Name	Description
	To delete the selected log from the Quick Log Viewer table.
	To clear all the logs from theQuick Log Viewer table.
	To save the log entries in the table to a file.
	To activate context-sensitive help.
	To set the number of logs to be maintained.

Chapter 17: Managing logs in the Quick Log Viewer

Setting the number of Quick Logs to manage

You can select the number of Quick Logs to be managed using the Quick Log Options button on the Quick Log Viewer toolbar. To set the number of logs:

1. In the Quick Log Viewer window, click  . The system displays the Quick Log Options dialog box.
2. Type a number from 100 through 5000.
   For example, if you want to manage 500 logs, type `500`.
3. Click **OK**.

Deleting logs

You can delete the entries in the Quick Log Viewer table.

To delete logs:

1. Select the line you want to delete. To choose multiple lines press `Ctrl` and select the lines you want to delete.
2. Click  to delete the selected logs permanently form the Quick Log Viewer table.

Clearing logs

You can clear all the entries from the Quick Log Viewer. To clear all the entries from the Quick Log Viewer table:

1. Click  . The system displays the Clear Log dialog box.
2. Click **OK** to clear the entries.

Saving logs

You can save all the entries in the Quick Log Viewer table into a Microsoft Excel CSV (Comma Separated Values) file. To save the file:

1. Click  . The system displays the Save dialog box.
2. Browse to the directory in which you want to save the file.
3. Enter a name for the file in the **File Name** field.
4. Click **Save** to save the logs to the specified file.

Chapter 18: Introduction to the Avaya NM Backup Utility

NM Backup Utility overview

The NM Backup Utility is used to back up multiple configuration files, database and application data of the Network Management Console, Provisioning and Installation Manager for Gateways, and Provisioning and Installation Manager for IP Office applications. You can choose to back up one or more applications as part of a backup job. This wizard helps you to setup a new backup job or edit an existing one.

You can run the backup job immediately or schedule it to run later. When the backup operation is complete, the utility creates a compressed archive and a text file with essential information about the contents of the archive. The text file is only for your convenience and is not needed during the restore operation. You can choose to store the backup archive on a FTP server or locally on the Network Management server while setting up the job.

The utility backs up various configuration files and application data which are essential to restore the Network Management server in case of an unrecoverable error. You need not recreate all the administered settings when you bring up the Network Management server. Instead you can restore the information from the backup archive stored on the Network Management or remote FTP server. If you are installing a Service Pack, it is recommended that you take a backup before installing the Service Pack.

For Network Management Console, back up includes discovery configurations, Network Map Definitions, Communication Manager server passwords and licensing information and various other files. The Network Management Console backup also includes the settings for the Secure Access Administration, Configuration Backup Restore and Software Update Manager applications.

The Provisioning and Installation Manager for Gateways, and Provisioning and Installation Manager for IP Office back up add their configuration files as well. The database back up includes the Network Management Console, AIM-Admin, PIM and User Admin databases.

Installation specific information such as SSO Configuration files, licensing information, IM application jobs, environment and binary files (software libraries etc.) are also bundled with the backup archive.

Launching the NM Backup Utility

You can launch the NM Backup Utility window from the Integrated Management Launch Page or from the Network Management Console window.

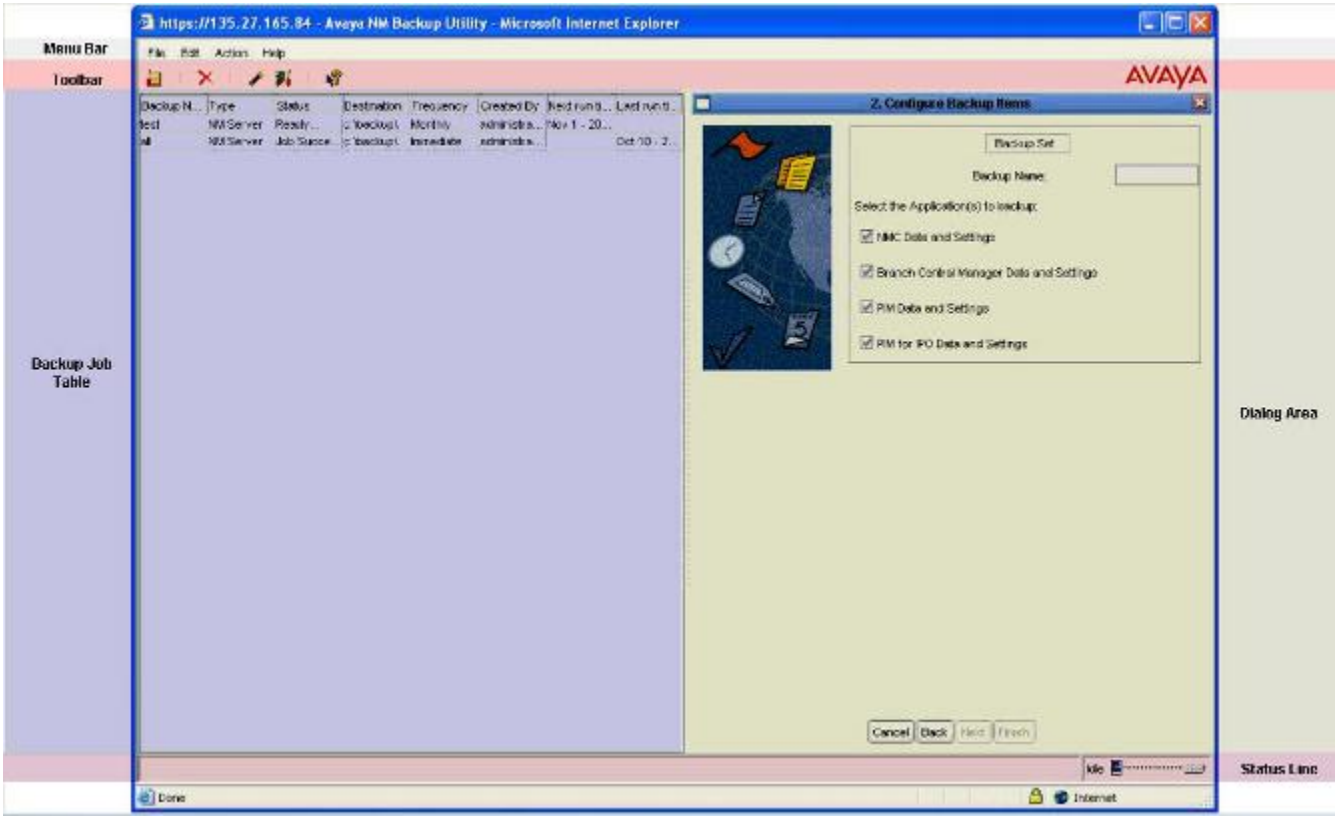
To launch the NM Backup Utility, do one of the following:

1. Click **NM Backup Utility** from the Integrated Management launch page.
2. Select **Tools** > **Avaya NM Backup Utility** from the Network Management Console window.

NM Backup Utility window

TheNM Backup Utility user interface consists of the following elements:

- Menu Bar – For more information on the NM Backup Utility menus, refer to Appendix A: Network Management Menus.
- NM Backup Utility toolbar on page 161 — Toolbar buttons for accessing the Backup Utility functions.
- NM Backup Job table on page 162 — Details of the jobs in queue are shown in a tabular format.
- NM Backup Utility dialog area on page 163 — A resizeable area where all dialog box open.
- NM Backup Utility Status Line on page 163 — Displays information about the current jobs in queue.



Related topics:

[NM Backup Utility toolbar](#) on page 161
[NM Backup Job table](#) on page 162
[NM Backup Utility dialog area](#) on page 163
[NM Backup Utility Status Line](#) on page 163

NM Backup Utility toolbar

The table describes the buttons on the NM Backup Utility toolbar and gives the equivalent menu options.

Button	Description	Menu Item
	Opens the NM Backup Utility Options dialog box.	**File** > **Options**
	Deletes the selected Backup Job from the NM Backup Utility table.	**Edit** > **Delete**
	Opens the NM Backup Utility Wizard dialog box.	**Actions** > **Backup**

Button	Description	Menu Item
	Opens the NM Backup Utility Wizard dialog box to edit the job. Please note you cannot edit jobs which are run immediately.	**Actions** > **Edit Backup**
	Open context–sensitive help.	**Help** > **Help On**

NM Backup Job table

The NM Backup Job table contains the details of the Backup Jobs that are in queue. The following table provides a list of the fields in the NM Backup Job table and provides and explanation of each field.

Name	Description
Backup Name	The Backup name as defined in the Configure Backup Items dialog box.
Type	The type of server on which backup is stored. The possible options are: • NM server • FTP server
Status	The status of backup is shown here. The possible values are: • Planned • Job Succeeded • Job Failed: Reason for failure
Destination	The destination where the backup archive is stored.
Frequency	The schedule selected while creating the backup job. The possible values are: • Immediate • Daily • Weekly • Monthly
Created By	The name of user who created the backup.
Next run time	The scheduled date and time for the next backup to be taken.
Last runtime	The date and time when the last backup was taken.

NM Backup Utility dialog area

The area to the right of the NM Backup Utility table is where all dialog boxes open. This area can be resized by dragging the horizontal splitter bar with the mouse. When a dialog box opens, it replaces the current dialog box open in the dialog area.

NM Backup Utility Status Line

The NM Backup Utility's Status Line displays the number of queued Backup jobs in the NM Backup Utility table. In addition, the Status Line displays the progress of the backup.

Configuring the default server parameters for backup

You can use the NM Backup Utility Options dialog box to configure the default Network Management and FTP server parameters for backup. These parameters are used as defaults while setting up a backup job. For more information on how to backup data, refer to Using the NM Backup Utility wizard on page 164

To configure the Server parameters:

1. Do one of the following:
   a. Click  .
   b. Select **File** > **Options** from thefrom the NM Backup Utility user Interface. The system displays the Options dialog box.
2. Enter the Server parameters in the Options dialog box.
3. Click **Apply** to save the parameters.

Related topics:

NM Backup Utility Options field descriptions on page 164

NM Backup Utility Options field descriptions

The following table provides a list of the fields in the Options dialog box of the NM Backup Utility.

Name	Description
FTP Server IP Address	IP address of the FTP server
FTP Port	The port number
UserName	FTP username
Password	FTP password
Retype Password	Re-enter the password in the **Password** field.
FTP Backup Directory Path	Absolute path of the directory where you want to save the backup archive on FTP server.
NM Backup Directory Path	Absolute path of the directory where you want to save the backup archive on Network Management server.

Using the NM Backup Utility wizard

The NM Backup Utility wizard can be used to backup configuration files and database files of the Network Management Console, Provisioning and Installation Manager for Gateways, and Provisioning and Installation Manager for IP Officeapplications.

To backup the data:

1. Do one of the following:
   a. Click  .
   b. Select **Action** > **Backup**. The system displays the NM Backup Utility wizard.
2. Click **Next**. The system displays the Configure Backup Items dialog box. Do the following:
   a. Enter a name for the Backup in the **Backup Name** field.

Note:

The name of the backup archive is formed as: “Backupname_MMMMM.dd.yyyy.HHmmss.” For example, if you enter the backup name as ‘test’ then the name of the backup archive is something like test_July.28.2008.123244.zip where the date and time reflects the date and time when the backup job runs.

b. Select the applications that you want to backup.

3. Click **Next**. The system displays the Select Backup Destination dialog box. By default, the parameters configured in the Options dialog box appear here. You can change the parameters if you want to save the backup to a different location.

Note:

If you did not set default parameters earlier, all the fields appear blank. You can enter the parameters in this screen. If you want to set these parameters as default values, click **Set as Defaults Options**.

4. Do one of the following in the Select Backup Destination dialog box.
   a. To enter or edit the Network Management server parameters:
      i. Select **NM Server**.
      ii. Enter/Edit the directory path where you want to save the backup in the **Target Directory** field.
   b. To enter or edit FTP Server parameter:
      i. Select **FTP Server**.
      ii. Enter/Edit the IP address of the FTP server in the **Host Address** field.
      iii. Enter/Edit the port number in the **Port** field.
      iv. Enter/Edit the directory path in the **Target Directory** field.
      v. Enter/Edit the FTP user name in the **FTP Login** field.
      vi. Enter/Edit the FTP password in the **Password** field.
5. Click **Next**. The system displays the Select Job Type dialog box. Do one of the following:
   a. To run the backup immediately:
      i. Select **Immediate**.
      ii. Click **Next**. The system displays the Summary dialog box.
   b. To run the job periodically:
      i. Select **Periodic**.
      ii. Click **Next**. The system displays the Schedule Backup Job dialog box.
      iii. Select the time when you want to start the backup from the **Start hour:** drop-down list under the **Job Start time** section of the dialog box.
      iv. Do one of the following under the **Recurrence Pattern** section of the dialog box:
         • If you want to schedule the backup daily, select **Daily**. If you want to schedule the backup at fixed intervals (days), enter a

value in the **Every day(s)** field. For example, If you want to schedule the backup every two days, enter `2`.

- If you want to schedule the backup weekly, select **Weekly**. Choose the day of the week on which you want to schedule the backup. If you want to schedule the backup to run on fixed intervals (weeks), enter a value in the **recur every week(s) on:** field. For example, if you want to schedule the backup every two weeks, enter `2`
- If you want to schedule the backup monthly, select **Monthly**. Type the day of the month on which you want to schedule the backup in the **Day of every month(s)** field. For example, if you want to schedule the backup to run on the first of every month enter `1`. If you want to schedule the backup to run at fixed intervals (months), enter a value in the **month(s)** field. For example, if you want to schedule the backup to run on day one after every two months then enter `1` in the **Day** field and `2` in **months(s)** field.

v. Click **Start Date** under the **Range of recurrence** section of the dialog box. The system displays the calendar. Select the start date for the backup.

vi. Do one of the following under the **Range of recurrence** section of the dialog box:

- If you want to end the schedule for backup after a fixed number of occurrences, select **End after occurrences**. Enter the number or occurrences in this field. For example, if you want to end the schedule after 15 occurrences, enter `15` in this field.
- If you want to end the schedule for backup on a particular date, select **End by** and then click **End Date**. The system displays a calendar. Select the end date.
- If you do not want to specify an end date for the schedule, select **No end date**. This is the default option.

6. Click **Next**. The system displays the Summary dialog box. The Summary dialog box displays the following information:

- **Backup Name** — This displays the name of the Backup you entered in the Configure Backup Items dialog box.
- **Application Types** — This displays the application you chose to backup in the Configure Backup Items dialog box.
- **Backup Destination** — This displays the backup destination you chose in the Select Backup Destination dialog box.

- **Schedule Information** — This displays the schedule information you chose in the Schedule Backup Job dialog box.

7. Click **Submit**. The wizard closes and a row is added for this backup job in the NM Backup job table.

   The job executes at scheduled intervals, and the progress percentage is updated in the status column. When the job is complete, the status column is updated with the message "`Job Succeeded. Stored in archive: test_July.28.2008.123244.zip`." If the job fails the status message says "`Job Failed: reason for failure`." When the job succeeds, the archive is created at the backup location you entered while setting up the backup job. You also find an additional text file at the location with same name of archive (for example, "test_July.28.2008.123244.txt") which lists the applications backed up in the archive, the Network Management version and other useful information for future reference. This text file is not required during restore. You can safely delete it if you want to. The archive need not be at the same location for restore to succeed and it is safe to move archive to different locations if required.

   Warning:

   Please do not modify the contents of the archive. Even if you just unzip and recompress the archive without any modifications, the restore may fail.

Editing a backup job using the NM Backup Utility

You can edit the backup jobs that are scheduled to run periodically.

Note:

You cannot edit the backup jobs that are run immediately.

To edit a backup job:

1. Select the job to edit from the NM Backup job table.
2. Click  or select **Actions** > **Edit Backup.** The system displays the Welcome dialog box.
3. Click **Next** and navigate to the dialog box where you want to edit.
4. Once you finish editing the job click **Submit** on the Summary dialog box to update the details in the NM Backup job table.

Chapter 19: Introduction to the Avaya NM Easy Restore Utility

NM Easy Restore Utility overview

The NM Easy Restore Utility is used to restore the backup taken by the NM Backup Utility. For more information on the NM Backup Utility, refer to NM Backup Utility overview on page 159

Note:

The restore can only be done on the same Network Management server from where the backup was taken.

Only Windows Administrators can restore the data.

Launching the NM Easy Restore utility

The NM Easy Restore utility can be launched only from the Network Management server.

To launch the NM Easy Restore Utility:

From the Network Management server, select **Start** > **All Programs** > **Avaya** > **Tools** > **NM Easy Restore**. The system displays the NM Easy Restore dialog box.

Restoring the data using the Avaya NM Easy Restore Utility

Restoring the backup file from the NM server

1. From the Network Management server, select **Start** > **All Programs** > **Avaya** > **Tools** > **NM Easy Restore.** The system displays the NM Easy Restore dialog box.
2. Select **NM Server**.
3. Click **Browse** and navigate to the directory where you saved the recent backup archive and select the backup archive.
4. Check **Recover PostgresSQL database using write ahead logs (WAL)** only if you have selected the most recent backup archive for restore.

   For more information on the **Recover PostgresSQL database using write ahead logs (WAL)**, refer to About Recovering the PostgresSQL database using write ahead logs (WAL) on page 171
5. Click **Restore** to start the restore operation. The status is updated in the log window. Once the restore operation is completed successfully, you can close the restore utility and start Avaya services from **Start** > **Program Files** > **Avaya** > **Start Avaya Services**.

Result

Note:

If Avaya Services are already running then it is stopped when you click Restore. You can start it after the restore operation is completed successfully.

Restoring the backup file from the FTP server

1. From the Network Management server, select **Start** > **All Programs** > **Avaya** > **Tools** > **NM Easy Restore.** The system displays the NM Easy Restore dialog box.
2. Select **FTP Server**.
3. The FTP parameters entered during the backup process are displayed.

4. Select the backup archive that you want to restore from the directory where you saved it.
5. Check **Recover PostgresSQL database using write ahead logs (WAL)** only if you have selected the most recent backup archive for restore.

   For more information on the **Recover PostgresSQL database using write ahead logs (WAL)**, refer to About Recovering the PostgresSQL database using write ahead logs (WAL) on page 171
6. Click **Restore** to start the restore operation. The status is updated in the log window. Once the restore operation is completed successfully, you can close the restore utility and start Avaya services from **Start** > **Program Files** > **Avaya** > **Start Avaya Services**.

Result

Note:

If Avaya Services are already running then it is stopped when you click **Restore**. You can start it after the restore operation is completed successfully.

About Recovering the PostgresSQL database using write ahead logs (WAL)

The **Recover PostgresSQL database using write ahead logs (WAL)** option is used to restore the PostgreSQL database to the current state with all the entries in it.

The Network Management Console use the PostgreSQL database to store the data. The database gets installed automatically during the Network Management installation. When you backup the data using the NM Backup Utility the data from the PostgreSQL database also gets backed up.

When you restore the backed up data using the NM Easy Restore utility, all the data entered in the database after the backup operation is not included in the restore. It is lost. However, it is possible to recover this data using the PostgreSQL database feature called WAL (Write Ahead log) archiving.

Using this feature, PostgreSQL remembers the date and time you took the last backup and all the data entered thereafter is maintained separately in a log file called “write ahead log” (WAL) in its internal directories.

During restore, if **Recover PostgresSQL database using write ahead logs (WAL)** is selected, the NM Easy Restore utility attempts to restore this data using the latest WAL file along with the backed up data bringing the database to the current state with all the entries in it.

Following conditions should be met for successful restore using the **Recover PostgresSQL database using write ahead logs (WAL)** option.

- The backup archive you restore from should be the latest backup taken. This is necessary because the current WAL files are with respect to the latest backup date and time. If you choose an old backup archive the entries in the WAL file can not be restored.
- The application should not be reinstalled after backup. If you reinstall the application anytime after backup, the WAL files stored by database get deleted and hence you are not able to restore the database in the current state. In such case, the database is restored to the same state as it was during backup. The restore utility does not report any error even if the WAL files are not in expected sequence.

Note:

You can use the NM Backup Utility to backup the data and settings of Network Management Console, Provisioning and Installation Manager for Gateways, and Provisioning and Installation Manager for IP Office applications. Of these only Network Management Console use the PostgreSQL database. **Recover PostgresSQL database using write ahead logs (WAL)** option has no significance for Provisioning and Installation Manager for Gateways and Provisioning and Installation Manager for IP Office applications restore.

Note:

Do not select the option **Recover PostgresSQL database using write ahead logs (WAL)** if the last restore attempt failed.

Appendix A: Network Management menus

Network Management includes the following menus:

- Avaya Network Management Console Menus
- Discovery Menus
- Event Log Browser Menus
- Event Configuration Menus
- Action List Menus
- NM Log Viewer Menus
- NM Backup UtilityMenus

Avaya Network Management Console Menus

This section gives the full structure of the menus in the AvayaNetwork Management Console. These menus include

Related topics:

Avaya Network Management Console File Menu on page 173
Avaya Network Management Console Edit Menu on page 174
AvayaNetwork Management Console View Menu on page 174
Avaya Network Management Console Actions Menu on page 175
Avaya Network Management Console Tools Menu on page 175
Avaya Network Management Console Help Menu on page 176

Avaya Network Management Console File Menu

Name	Description
New	Creates a new Network Object - Map, View, Branch, or Device.
Open map	Opens a Network map.
Save map	Saves a Network map.
Delete map	Deletes a Network map
Import map	Imports device information from a CSV file into the current Network map.

Name	Description
Export map	Exports device information from the current Network Map to a CSV file.
Print	Prints the current Network map.
Print Preview	Opens the Print Preview window for the Network map.
Options	Opens the Options dialog box.
Logout	Ends the current user's session.
Exit	Closes Network Management Console.

Avaya Network Management Console Edit Menu

Name	Description
Modify	Opens the Modify dialog box for the selected object.
Delete object	Deletes the selected object from the Network Map.
Modify View	Opens the Modify View dialog box.
Delete View	Deletes the current custom view.
Cut object	Cuts the selected object in a custom view to the clipboard.
Paste object	Pastes the object from the clipboard into a custom view.
Manage object	Manages a currently unmanaged Network Object.
Unmanage object	Unmanages a currently managed Network Object.
Find	Opens the Find dialog box.

AvayaNetwork Management Console View Menu

Name	Description
Connections/Endpoints	Opens the Port Connections/Registered Endpoints log.
Inventory	Opens the Inventory log.
Tooltip	Switch the display of device tooltips.

Avaya Network Management Console Actions Menu

Name	Description
Avaya Secure Access Administration	Opens the Security Access Administraton.
Avaya User Administration	Opens Avaya User Administration.
Change Password	Opens the Change Password dialog box.
Event Manager	Opens the Event Log browser.
NM Log Viewer	Opens the NM Log Viewer.
IP Discovery	Opens the Discovery window.
Network Discovery Wizard	Opens the Network Discovery Wizard.
Get Write Permission	Request read/write permission for your console session.
Release Write Permission	Release read/write permission for your console session.

Avaya Network Management Console Tools Menu

Name	Description
Voice Applications	Provides access to the following submenus: • Site Administration — Connects to the switch controlling a supported voice device and opens the appropriate form. • Avaya MultiSite Administration — Launches the Avaya MultiSite Administration. • Avaya Avaya Fault and Performance Manager — Launches the Avaya Avaya Fault and Performance Manager. • Avaya Voice Announcement Manager — Launches the Avaya Voice Announcement Manager .
Avaya Software Update Manager	Launches the Avaya Software Update Manager.
Avaya Provisioning and Installation Manager	Launches the Avaya Provisioning and Installation Manager for Gateways.

Name	Description
Avaya Provisioning and Installation Manager for IPO Devices	Launches Avaya Provisioning and Installation Manager for IP Office Devices.
Avaya SMON Manager	Launches the Avaya SMON Manager.
Avaya Device Manager	Launches the Device Manager for the selected device.
Avaya NM Backup Utility	Launches the NM Backup Utility wizard.
Avaya Configuration Backup Restore	Launches the Avaya Configuration Backup Restore.
Polycom GMS	Launches the Polycom GMS for the selected Polycom device.
Extreme EPICenter	Launches the Extreme EPICenter for the selected Extreme device.
IP Office Manager	Launches IP Office Manager.
Avaya easy Management	Launches the Avaya easy Management.
IP Office System Status	Launches IP Office system status.
G860/Audio Codes Mediant 3000 EMS Client	Launches the G860/Audio Codes Mediant 3000 EMS client
Web	Launches a Web session to the selected device.
Telnet	Launches a Telnet session to the selected device.
Ping	PINGs the selected device.
SSH	Launches a SSH session to the selected device

Avaya Network Management Console Help Menu

Name	Description
Contents	Opens the on-line help to the contents page.
Help On	Activates the context-sensitive help.
About Avaya Network Management Console	Opens the About dialog box showing the copyright and version information for the AvayaNetwork Management Console.

Discovery Menus

This section gives the full structure of the menus in the Discovery window.

Related topics:

Discovery File Menu on page 177
Discovery Edit Menu on page 177
Discovery View Menu on page 178
Discovery Actions Menu on page 178
Discovery Help Menu on page 178

Discovery File Menu

Name	Description
Save changes	Saves the updated Network Map with the results of the latest Discovery to the database.
Options	Opens the Discovery Options dialog box.
Exit	Closes the Discovery window.

Discovery Edit Menu

Name	Description
Add	Opens the Add Subnet dialog box.
Modify	Opens the Modify Subnet dialog box.
Select	Selects the **Discover** field for the selected subnets.
Unselect	Clears the **Discover** field for the selected subnets.
Delete	Deletes the selected subnet from the Subnets table.
Delete All	Deletes all subnets from the Subnets table.

Discovery View Menu

Name	Description
Discovery Log	Switch the display of the Discovery log.

Discovery Actions Menu

Name	Description
Start Network Discovery	Starts a Discovery based on the contents of the Subnets table.
Stop Network Discovery	Stops the Discovery process.
Schedule Network Discovery	Opens the Scheduler dialog box.
Discover Interfaces	Select the check box if you want to discover interfaces.

Discovery Help Menu

Name	Description
Contents	Opens the on-line help to the first topic.
Help On	Activates the context-sensitive help.

Event Log Browser Menus

This section gives the full structure of the menus in the Event log browser.

Related topics:

Event Log Browser File Menu on page 179
Event Log Browser Edit Menu on page 179
Event Log Browser View Menu on page 179
Event Log Browser Help Menu on page 180

Event Log Browser File Menu

Name	Description
Options	Opens the Trap log Options dialog box.
Export	Saves the Event log to a file.
Exit	Closes the Event log.

Event Log Browser Edit Menu

Name	Description
Delete	Deletes the selected traps.
Acknowledge	Acknowledges the selected traps.
UnAcknowledge	Unacknowledges the selected traps.
Modify Event	Opens the Modify Event dialog box.
Select All	Select all traps visible in the Trap table.
Delete All	Deletes all the traps in the Trap log.
Change Severity > Change severity to Info	Changes the severity of the selected traps to Info.
Change Severity > Change severity to Warning	Changes the severity of the selected traps to Warning.
Change Severity > Change severity to Minor	Changes the severity of the selected traps to Minor.
Change Severity > Change severity to Major	Changes the severity of the selected traps to Major.
Change Severity > Change severity to Critical	Changes the severity of the selected traps to Critical.

Event Log Browser View Menu

Name	Description
Filter > Severity Filter	Opens the Severity Filter dialog box.

Name	Description
Filter > Category Filter	Opens the Category Filter dialog box.
Filter > IP Address Filter	Opens the IP Address Filter dialog box.
Filter > Device Type Filter	Opens the Device Type Filter dialog box.
Filter > Acknowledge Filter	Opens the Acknowledged Filter dialog box.
Filter > No Filter	Displays all events in the Trap table.
Filter > New Traps on top	Displays the newest traps at the top of the list in the Event log browser table.

Event Log Browser Help Menu

Name	Description
Contents	Opens the on-line help to the first topic.
Help on	Activates the context-sensitive help.

Event Configuration Menus

This section gives the full structure of the menus in the Event Configuration window.

Related topics:

Event Configuration File Menu on page 180
Event Configuration Edit Menu on page 181
Event Configuration Tools Menu on page 181
Event Configuration Help Menu on page 181

Event Configuration File Menu

Name	Description
Exit	Closes the Event log.

Event Configuration Edit Menu

Name	Description
Modify Event	Opens the Modify Event dialog box.
Delete All	Deletes all the traps in the Trap log.

Event Configuration Tools Menu

Name	Description
Action List	Opens the Action List window.
Event Forwarding	Opens the Event Forwarding Options dialog box.

Event Configuration Help Menu

Name	Description
Contents	Opens the on-line help to the first topic.
Help on	Activates the context-sensitive help.

Action List Menus

This section gives the full structure of the menus in the Action List window.

Related topics:

Action List File Menu on page 182
Action List Edit Menu on page 182
Action List Tools Menu on page 182
Action List Help Menu on page 182

Action List File Menu

Name	Description
Exit	Closes the Action List.

Action List Edit Menu

Name	Description
Apply	Applies the changes to the Action List to the network.
Revert	Undoes all unapplied changes.
Add	Opens the Add Action dialog box.
Modify	Opens the Modify Action dialog box.
Delete All	Deletes all the traps in the Trap log.
Delete	Deletes the selected actions.

Action List Tools Menu

Name	Description
Options	Opens the Action List Options dialog box.

Action List Help Menu

Name	Description
Contents	Opens the on-line help to the first topic.
Help On	Activates the context-sensitive help.

NM Log Viewer Menus

This section gives the full structure of the menus in the NM Log Viewer browser.

Related topics:

NM Log Viewer File Menu on page 183
NM Log Viewer Edit Menu on page 183
NM Log Viewer View Menu on page 183
NM Log Viewer Help Menu on page 184

NM Log Viewer File Menu

Name	Description
Open	To open a previously saved log file.
Export	Saves the logs displayed in the Log table to a file. You can save the files in CSV or XML format.
Exit	Closes the NM Log Viewer.

NM Log Viewer Edit Menu

Name	Description
Select All	Select all logs visible in the NM Log Viewer table.
Copy	Copies selected logs.

NM Log Viewer View Menu

Name	Description
Filter > **Severity Filter**	Opens the Severity Filter dialog box.
Filter > **No Filter**	Cancel the current filtering option and view all logs in the NM Log Viewer table.

NM Log Viewer Help Menu

Name	Description
Contents	Opens the on-line help to the first topic.
Help on	Activates the context-sensitive help.

NM Backup Utility Menus

This section gives the full structure of the menus in the NM Backup Utility browser.

Related topics:

NM Backup Utility File Menu on page 184
NM Backup Utility Edit Menu on page 184
NM Backup Utility Action Menu on page 185
NM Backup Utility Help Menu on page 185

NM Backup Utility File Menu

Name	Description
Options	To open the NM Backup Utility Options dialog box to configure default Network Management or FTP Server parameter.

NM Backup Utility Edit Menu

Name	Description
Delete	To delete a selected backup job from the table.

NM Backup Utility Action Menu

Name	Description
Backup	To open the NM Backup Utility wizard
Edit Backup	To edit the Backup job selected from the NM Backup Utility table.

NM Backup Utility Help Menu

Name	Description
Contents	Opens the on-line help to the first topic.
Help on	Activates the context-sensitive help.

Appendix B: Enhancement introduced in previous releases

Enhancement introduced in Release 5.2 Service Pack 3

The AvayaIntegrated Management Network Management Release 5.2 Service Pack 3 introduces the following enhancements in the Network Management Console application.

- The following name changes are done to applications in the Avaya Integrated Management product.

Old Name	New Name
Enterprise Network Management	Network Management
Avaya Communication Manager	Avaya Aura® Communication Manager
Avaya Aura®Communication Manager Branch Edition	Avaya Aura®Communication Manager Branch
Communication Manager Branch Edition - Central Manager	Branch Central Manager
Configuration Backup and Restore Manager	Configuration Backup Restore
System Management	Performance and Administration
Administration Tools	Site Administration
ENM Backup Utility	NM Backup Utility
ENM Easy Restore	NM Easy Restore
ENM Log Viewer	NM Log Viewer

- Support for Avaya Aura®Communication Manager Release 5.2.1. Network Management Console supports the following functions on Communication Manager Release 5.2.1:
  - Discovery and display of devices in the Device Type view
  - Proper correlation of devices in the VoIP System View
  - Basic administration tasks such as Adding, Deleting, and Modifying devices
  - Network Discovery Wizard

- This release supports Avaya Aura®Communication Manager running on the Next Gen S8800 server platform in simplex and duplex modes.
  - Support for the new platform Next Gen S85xx server - Support for the new platform Next Gen S87xx server
  - Support for the new platform Next Gen S87xx server

Note:

In the simplex mode, the Network Management Console displays the S8800 as S85XX, and in the duplex mode as S87XX.

- This release reinstates the IP Office support similar to the Network Management Release 5.0. Specifically, this release provides IP Office 5.0 support in the following applications:
  - Discovery, including VoIP SystemView
  - Port Connections
  - Secure Access Administration
  - Fault Monitoring
  - Software Update Manager
  - Provisioning and Installation Manager for IP Office
  - IP Office System Status
- Support for IP Office in theNM Backup Utility and the NM Easy Restore Utility

  This release supports backup and restore of the IP Office related files using the NM Backup Utility and theNM Easy Restore Utility tools. The NM Backup Utility also saves the configuration files of Provisioning and Installation Manager for IP Office.
- Support for IP Office Manager 7.0

  You can start IP Office Manager 7.0 on an IP Office device to see detailed information not presented in the System View. A new instance of IP Office Manager opens each time you start the application from the Network Management Console.
- G860 related changes:
  - The G860 AudioCodes SysOID is replaced by Avaya SysOID.
  - The G860 AudioCodes Trap OIDs is replaced by Avaya Trap OIDs.
- Support for Microsoft Windows Vista with Service Pack 2
- In this release, the sequence of the discovery process has changed. This helps in enhancing the speed of the IP Phone data discovery. The new discovery sequence is:
  a. IP discovery
  b. System View discovery
  c. IP phone data discovery
  d. Port connection discovery
- In this release, the **Discover** check box in the Network Management Console's **File** > **Options** > **CM Servers Password** tab has been renamed to **Discover Phones**. The label **Discover**, was misleading. This check box is used to discover phones associated with

the Avaya Aura®Communication Manager. Even if you do not select the check box, the Communication Manager is discovered and displayed in the Network Management Console view.

Note:

The state of the check box does not affect Software Update Manager's operation.

- From this release, you can configure a maximum of five user defined applications or tools link to appear on the Integrated Management launch page.

  To add links:

  a. In the Network Management Server, select **Start** > **All Programs** > **Avaya** > **Tools** > **Configure Avaya Integrated Management**.
  b. Click the **Other URL Information** tab.
  c. In the **Name** field, enter the name of the application or tool you want to add to the launch page.
  d. In the **URL:** field, enter the URL of the application or tool.
  e. Click **Save**.
  f. Click **Exit**. You can view the link on the Integrated Management launch page under the section, **User Defined Operations and Links**.

Note:

For information on the problems fixed in this release, refer to the *Avaya Integrated Management - Network Management Release 5.2 Service Pack 3 Release Notes* available on the Avaya Support Web site.

Enhancements introduced in Release 5.2 Service Pack 2

For information on changes delivered to the Avaya Integrated Management - Enterprise Network Management Release 5.2 Service Pack 2, refer to *Integrated Management - Enterprise Network Management Release 5.2 Service Pack 2 Release notes* available on the Avaya Support web site.

Enhancements introduced in Release 5.2 Service Pack 1

For information on changes delivered to the Avaya Integrated Management - Enterprise Network Management Release 5.2 Service Pack 1, refer to *Integrated Management* -

Enterprise Network Management Release 5.2 Service Pack 1 Release notes available on the Avaya Support web site.

Enhancements introduced in Avaya Integrated Management Release 6.0 Service Pack 2

The Avaya Network Management Console Release 5.2 introduced the following enhancements:

- Support for the Communication Manager Release 5.2

  You can automatically configure the Communication Manager Release 5.2 to work with the Avaya Network Management Console. All digital and analog phones that work with the Communication Manager Release 5.2 are discovered and displayed in the Avaya Network Management Console console.

- Support for S8300D

  Support for the following functions of the Communication Manager running on an S8300D:

  - Auto discovery and manual addition
  - Modify and delete operations
  - Fault monitoring
  - Ping and Telnet operations

- Support for S8400 as an ESS

  The Network Management Console System View discovery process handles S8400 devices in the same way as supported in the Network Management Console Release 5.0, with the addition that S8400 devices can also be handled as an Enterprise Survivable Server (ESS) in addition to being a Communication Manager main server.

- Support for the G430 Media Gateway

  Support for the following functions of the G430 Media Gateway:

  - Automatic Discovery of a G430 by the Network Discovery Wizard
  - Manual addition of a G430 device
  - Display of discovered and manually added G430 in the Subnet view and the Device Type view
  - The Network Management Console System View discovery associates the G430 with its Communication Manager and endpoints.
  - Add, Modify and Delete administration operation on the G430 device

- Port connection table displays for the G430 in the same manner as for the G450 device
- Option to launch the following management applications in the context of selected G430 device:
  - Device Manager
  - Web interface
  - Telnet
  - Voice applications like Site Administration, Avaya MultiSite Administration, Avaya Fault and Performance Manager, and Avaya Voice Announcement Manager
- Display of SNMP notifications generated by the G430 in the Network Management Console Event log
- The Network Management Console supports new traps for the G430 media gateway, EM200 expansion modules and new Media Modules MM714B and MM118
- The Network Management Console fault monitoring service monitors the G430 devices for faults in the same manner as the G450 device.

• Support for new Extreme devices

The following new Extreme devices are supported in this release:

- Summit X150-24t
- Summit X150-48t
- Summit X150-24p
- Summit WM 200
- Summit WM 2000

The Network Management Console supports the following functions of the new Extreme devices:

- The Network Management Console provides the option to select the new Extreme device types among the device types to be discovered by the Network Management Console network discovery. The new Extreme device types are selected by default in the device types list for discovery.
- The Network Management Console displays discovered as well as manually added new Extreme devices in the Subnet View and the Device Type View.
- The Network Management Console supports Add, Modify and Delete administration operations on the new Extreme devices.

• Support for Communication Manager Branch Edition (formerly known as Distributed Office) Release 2.0

The Network Management Console provides the option of selecting the following Telephony devices to be discovered by the Network Management Console network discovery:

- Communication Manager Branch Edition G430 Media Gateway
- Communication Manager Branch Edition G450 Media Gateway
- Communication Manager Branch Edition G430 Telephony Server
- Communication Manager Branch Edition G450 Telephony Server

The Network Management Console supports Add, Modify and Delete administration operations on the G430 and G450 Telephony Server devices.

The Network Management Console displays the G430 and G450 Telephony Servers under Communication Manager Branch Edition branch in the System View.

The Network Management Console supports trap formatting and Alarm MIB for the G430 and G450 Telephony Server device.

The Network Management Console displays phones connected to the G430 and G450 Telephony Server in the Port connection table.

• Support for setting Syslog Server parameters

Now with the Enterprise Network Management, you can choose to log important events and activities performed within the Enterprise Network to a Syslog host (a server or machine that receives syslog messages). This enables a centralized logging location where multiple instances of the Enterprise Network Management can log their activities.

The Syslog Server tab of the Avaya Network Management Console Options dialog box lets you configure the syslog servers where logs are logged. You can configure one or multiple syslog hosts.

• Support for setting Security Banner text

The Security Banner is launched once the Network Management Console applet is loaded. The Security Banner tab of the options dialog box lets you change or edit the text on the Security Banner. You can also choose to not display the Security Banner once the Network Management Console applet is loaded.

• Support for Quick Log Viewer

The Network Management Console keeps a log of important events and activities performed within the Enterprise Network. The Quick Log Viewer allows you to quickly view the important events taking place in the system. You can use the Quick Log Viewer to view all these activities.

• Support for I55 software and traps

- The Network Management Console supports the new version of I55 software the same way it was supported in release 5.0

- The Network Management Console supports formatting of new traps of I55 software in the NFaultMon application.
- The Network Management Console displays the new traps with proper description in the Event Manager Applications.

• Support for Mozilla Firefox 3.0 web browser

• Support for the following new variants of G860:

- G860 Mediant 5000
- G860 Mediant 8000

Support for the following functions for G860 Mediant 5000 and G860 Mediant 8000:

• Auto discovery and manual addition

• Modify and delete operations

• Fault monitoring including Alarms Tab (RFC 3877 – ALARM MIB)

• Ping and Telnet operations

-

• Support for the following new variants of Audio Codes gateways

Mediant 3000 (M3K)

Support for the following functions for Mediant M3K:

• Auto discovery and manual addition

• Modify and delete operations

• Fault monitoring including Alarms Tab (RFC 3877 – ALARM MIB)

• Ping and Telnet operations

• Support 16CC and 9640 SIP Phones

• Support for PE Duplex Server

• Support for SSH-2

The program SSH-2 (Secure Shell) provides an encrypted channel for logging into another device over a network, executing commands on a remote device, and moving files from one device to another. SSH-2 provides strong host-to-host and user authentication as well as secure encrypted communications over an insecure Internet. Rather than validating identities using passwords, SSH-2 uses public key encryption to authenticate remote hosts. All the tools in Integrated Management use SSH-2.

Using the Network Management Console Release 5.2 you can launch the following new applications introduced in this release.

• ENM Backup Utility

The Enterprise Network Management (ENM) Backup Utility wizard is used to back up multiple configuration files and databases of the Network Management Console (NMC),

Provisioning and Installation Manager (PIM) and Communication Manager Branch Edition Central Manager (formerly known as Distributed Office Central Manager) applications. The ENM Backup Utility allows you to store the backup of configuration files and database on the ENM server or on a remote FTP server. The backup operation can take place immediately or can be scheduled.

- ENM Easy Restore Utility

  The ENM Easy Restore Utility is used to restore the backup taken by the ENM Backup Utility. You can enter the path of the backup archive stored either on the ENM or FTP server to restore the data present in it.

- ENM Log Viewer

  The ENM Log Viewer is used to display log files generated by the Enterprise Network Management applications in a user friendly tabular format. The log file contains information about actions performed and events taking place in the Enterprise Network Management Offer.

Index

A

Acknowledging traps 133
Action
  audio files 139
  fields 137
  form area 127
  options 140
  scripts 137, 138
  table 127
Action list
  applying changes 139
Action List
  Edit menu 182
  File menu 182
  Help menu 182
  menus 181
  toolbar 126
  Tools menu 182
  user interface 125
actions
  deleting 139
Actions
  adding 136
  modifying 136
  overview 135
Adding
  actions 136
  devices to the database 76
  subnets 110
Alarms Table 32, 72–74
  choose parameters to view 73
  filtering 73
  overview 74
  parameters 74
  toolbar 72
  viewing 74
Application Launcher 59
Applying changes to the action list 139
Assign action
  fields 123
Assign Action Form 123
Assigning actions to events 140
Audio files 139
Avaya Fault and Performance Manager, launching 65
Avaya Multisite Administration, launching 64
Avaya Network Management
  Overview 13
  Terms 14
avaya network management console 29
Avaya Network Management console
  starting a remote session 27
Avaya Network Management Console
  Actions menu 175
  custom views 53
  Edit menu 174
  File menu 173
  help 47
  Help menu 176
  menus 173
  options 35
  overview 16
  status bar 33
  tables 46
  Tools menu 175
  user interface 29
  View menu 174
Avaya Network Management Console—l
  starting 27
Avaya Network Management server
  introduction 23
Avaya Network Management Server
  overview 15
  starting 23
  status 23
  status;.i.Starting, Avaya Network Management Server 23
  stopping 24
Avaya Site Administration, launching 63
Avaya Site Administrator, launching 63
Avaya Voice Announcement Manager, launching 65

B

backup
  editing a backup job using the NM Backup Utility 167

C

Change Password 29
Clearing

discovery log 115
Closing
discovery 100
Closing the event manager 127
Configuration Wizard
overview 91
Configuring
discovery method and range 103
discovery options 103
discovery's naming method 105
event forwarding 142
event forwarding recipients 143
events 140
router access parameters 113
SMTP server 140
Connectivity polling 40
Creating
custom views 54
Creating, Network Map 85
CSV File Structure 88
Custom Views 53–56
creating 54
deleting 55
deleting branches 56
modify 54
modifying branches 56

D

Database
adding devices 76
printing 57
deleting
actions 139
devices 78
error messages from the discovery log 115
logs 157
traps 134
Deleting
custom views branches 56
devices 78
subnets 112
Determining best names 105
device
type view 50
Device
manager 60
modifying parameters 76
parameters 77
device applications launching 59
Dialog area
discovery 99
Dialog area, Avaya Network Management Console 32
discovering
all subnets and nodes 108
nodes on a specific subnets 109
subnets already in the network map 115
subnets and nodes 108
your network 101
discovery 17, 100, 112, 115
deleting error messages from the discovery log 115
log area 100
overview 17
status bar 100
Discovery
Actions menu 178
closing the window 100
configuring method and range 103
configuring naming method 105
dialog area 99
File menu 177
log 113
menus 177
method 103
range 103
saving the log 114
scheduling 107
selecting device types 106
setting options 103
starting 97
toolbar 98
View menu 178
Discovery Log
clearing 115

E

E-mail settings 140
editing
backup job using NM Backup Utility 167
editing severity levels 134
eeleting
custom views 55
enhancements introduced in Avaya Integrated Management - Enterprise Network Management Release 5.2 Service Pack 1 189
enhancements introduced in Avaya Integrated Management - Enterprise Network Management Release 5.2 Service Pack 2 189
enhancements introduced in Avaya Integrated Management Release 5.2 190
Event configuration

Edit menu 181
File menu 180
Help menu 181
menus 180
toolbar 122
Tools menu 181
Event Configuration
form area 124
Event configuration, User Interface 121
Event forwarding
configuring 142
configuring recipients 143
sources 142
event handling
overview 18
Event Log
options 129
Event log browser
Edit menu 179
File menu 179
Help menu 180
menus 178
status line 121
toolbar 119
user interface 118
View menu 179
Event manager
closing 127
overview 117
user interface 118
viewing 117
Event table 123
Events
assigning actions to 140
configuring 140
exporting Communication Manager server passwords . . 43
exporting passwords 43
exporting the Network Map to database 88

F

fatabase
importing devices 87
Fields
action 137
action table 127
event table 123
network table 69
Fields, Alarms Table 74
filter
inventory table 84
port inventory table 84
filtering
alarms table 73
interfaces table 73
logs 149
logs by security level 149
modules table 73
port connections table 73
registered endpoints table 73
filtering traps
by IP address 131
by severity level 130
Filtering traps 130–132
by acknowledged 132
by device type 132
by IP address 131
Form area
action 127
Form Area, Assign Action 123
from the FTP server 170
from the NM server 170

G

G860 Devices 60

H

Help
using 47
how to
delete actions 139
delete devices 78
delete error messages from the discovery log 115
delete traps 134
discover all subnets and nodes 108
discover nodes on a specific subnet 109
edit severity levels 134
export Network Map to CSV files 88
filter port inventory table 84
filter tables 73
filter traps by IP address 131
filter traps by severity level 130
import devices into the database 87
refresh the network map 115
How to
acknowledge traps 133
add actions 136
add devices to the database 76
apply changes to the actions list 139

assign actions to events 140
choose inventory parameters to display 84
choose port inventory parameters to display 84
choose which table parameters to display 73
close the event manager 127
configure discover range 103
configure discovery method 103
configure discovery range 103
configure discovery's naming method 105
configure event forwarding 142
configure events 140
configure forwarding recipients 143
configure router access parameters 113
delete subnets 112
filter inventory table 84
filter traps 130
filter traps by acknowledged 132
filter traps by device type 132
filter traps by IP address 131
launch a web session 67
launch avaya fault and performance manager 65
launch avaya multisite administration 64
launch Avaya Site Administration 63
launch avaya site administrator 63
launch avaya voice announcement manager 65
launch device manager 60
launch polycom GMS 66
launch Telnet 61
launch web session 61
manually add subnets 110
modify actions 136
modify device parameters 76
modify subnets 111
print the network map 57
save the discovery log 114
save the trap table 135
schedule discovery operation 107
search for a device 57
select default Network Map 41
select device types to discover 106
select event forwarding sources 142
set action options 140
set connectivity polling 40
set discovery options 103
set IP SNMP access parameters 39
set SNMP access parameters 36
set SNMP access parameters for IP ranges 38
set SNMP default access parameters 37
start a remote session of Avaya Network Management console 27
start Avaya Network Management console 27
start Avaya Network Management server 23
stop Avaya Network Management server 24
switch views 49
use Avaya Network Management console help 47
use the discovery log 113
use tool tips 33
view all traps 133
view the event manager 117

I

importing Communication Manager server passwords ..43
importing devices into the database 87
importing passwords 43
interfaces 112
discovering 112
Interfaces Tab 32, 69
viewing the network table 69
Interfaces Table
choose parameters to view 73
filtering 73
toolbar 72
Introduction
Avaya Network Management server 23
Introduction, Network Tree 49
Inventory Table 81, 82, 84
choose parameters to view 84
filter 84
parameters 82
toolbar 82
IP Disocovery process 102

L

launch 145, 169
Launch 153
launch SSH session 62
Launching
avaya fault and performance manager 65
avaya multisite administration 64
Avaya Site Administration 63
avaya site administrator 63
avaya voice announcement manager 65
device manager 60
polycom GMS 66
Telnet 61
web session 61
launching Device Applications 59
Log Area

discovery 100
logs
deleting 157
filtering 149
save 158

M

Managing Objects 75
Manually adding subnets 110
Modifying
actions 136
custom views 54
custom views branches 56
device parameters 76
subnets 111
Modules Table 32, 72, 73, 75
choose parameters to view 73
filtering 73
parameters 75
toolbar 72
viewing 75

N

network
discovering 101
Network Management menus 173
Network Map
creating 85
exporting devices to CSV file 88
managing objects 75
opening 86
overview 17
printing 86
saving 86
selecting default 41
Network Map, Printing 57
Network Maps
Introduction 85
Network Table 32, 69, 71
alarms table 32
colors 71
fields 69
interfaces tab 69
modules table 32
Network tree 49
Network view area, using 69, 81
Network-wide applications 67
NM Backup Utility
Action menu 185
Edit menu 184
editing a backup job 167
File menu 184
Help menu 185
menus 184
NM Backup Utility Options Dialog Box Parameters 163
NM Easy Restore 169
NM Log Viewer 145, 183, 184
Edit menu 183
File menu 183
Help menu 184
NM on a Microsoft Windows OS supporting UAC 24

O

Once you choose the options to schedule the job click Next. The Summary dialog box opens. 164
Opening
network map 86
Opening the Discovery window 97
Opening the Network Discovery Wizard 91
Options
avaya network management console 35
discovery 103
event log 129
overview
event manager 117
Overview
actions 135
avaya network management 13
configuration wizard 91
network maps 85

P

parameters
device 77
Parameters
alarms table 74
modules table 75
port connections table 79
registered endpoints table 80
subnet 111
Password Change 29
Permissions
read only 34
read/write 34
setting defaults 41, 42
PINGing devices 62
Polycom GMS, launching 66

Port Connections Table
choose parameters to view 73
filtering 73
parameters 79
toolbar 72
Port Connections table, viewing 79
Port Inventory Table 81, 82, 84
choose parameters to view 84
filter 84
parameters 82
toolbar 82
Postgres database
adding devices 76
importing devices 87
what is 14
Postgres Database
printing 57
Printing
network map 86
Printing the network map 57

Q

Quick Log Viewer 153

R

Read/Write Defaults, Setting 41, 42
Refreshing the network map 111
Registered Endpoints Table
choose parameters to view 73
filtering 73
parameters 80
toolbar 72
viewing 80
Remote Access
security 28
Requesting write permissions 34
restoring 170
Restoring 170

S

Saving
network map 86
the discovery log 114
trap table 135
Scheduling, Discovery Operation 107
search
inventory table 84
port inventory table 84
Search
port connections table 73
registered endpoints table 73
Searching the tree view 57
Security
remote access 28
web browser access 28
Selecting
device types to discover 106
elements 46
set security banner text 44
Setting Read/Write Defaults 41, 42
severity levels, editing 134
SNMP access parameters
configuring 36
default parameters 37
IP ranges 38
specific IP parameters 39
Sources of events to forward 142
specifying a subnet to discover 109
Starting
avaya network management console 27
Status bar
discovery 100
Status Bar, User Interface 33
status line, event log browser 121
Stopping Avaya Network Management Server 24
Subnet
deleting 112
parameters 111
table 99
view 50
subnets and Nodes
discovering 108
Supported G860 Devices 60
syslog server parameters 45

T

Table
row status, deleted 46
row status, modified 46
row status, new entry 46
subnets 99
Tables
avaya network management console 46
Telnet 61
toolbar
discovery 98
event configuration 122
event log browser 119
Toolbar 30, 72, 82, 126

action list 126
alarms table 72
interfaces table 72
modules table 72
port connections table 72
port inventory table 82
registered endpoints table 72
Tooltips 33
Trap fields 120
Trap table
fields 120
saving 135
traps
deleting 134
Traps
acknowledging 133
filtering 130
viewing 133
viewing all 133
Tree view 32, 49, 57
searching 57

U

User Administration
Actions menu 178
user interface
event configuration window 121
event log browser 118
event manager 118
user Interface
network table 32
User interface
action list 125
User Interface 29, 30, 32, 33
alarms table 32
dialog area 32
modules table 32
status bar 33
toolbar 30
tooltips 33
tree view 32
Using
action scripts 137, 138
Avaya Network Management console help 47
registered endpoints table 80
the discovery log 113
the network view area 69, 81
the port connections table 79
using NM on a Microsoft Windows OS supporting UAC 24

V

view
device type 50
View
parameters in alarms table 73
parameters in interfaces table 73
parameters in inventory table 84
parameters in modules table 73
parameters in port connections table 73
parameters in port inventory table 84
parameters in registered endpoints table 73
subnet 50
VoIP system view 51
viewing 81
Viewing
modules table 75
the event manager 117
traps 133
VoIP system view 51

W

Web Browser
secure access 28
Web session 67
Web Session 61
What's New 20
who should use this manual 11